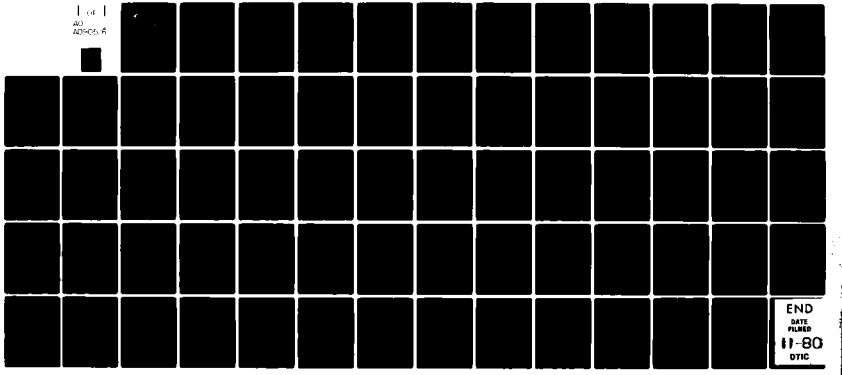
AD-A090 526 ELECTRONICS ENGINEERING GROUP (1842ND) SCOTT AFB IL F/G 9/2
FAULT-ISOLATION IN AIR FORCE BASE LEVEL DATA NETWORKS.(U)
SEP 80 T H WEAVER
UNCLASSIFIED 1842 EEG/EEIC-TR-80-7 NL



END
DATE FILMED
11-80
DTIC

1842EEG/EEIC TR 80-7

0

AFCC TECHNICAL REPORT

FAULT-ISOLATION IN AIR FORCE BASE LEVEL DATA NETWORKS

BASE TELEPROCESSING SYSTEMS
BASE COMMUNICATION SYSTEMS BRANCH
ELECTRONIC AND BASE SYSTEMS ENGINEERING DIVISION
1842 ELECTRONICS ENGINEERING GROUP (AFCC)
SCOTT AIR FORCE BASE, ILLINOIS 62225

10 SEPTEMBER 1980

1842 ELECTRONICS ENGINEERING GROUP

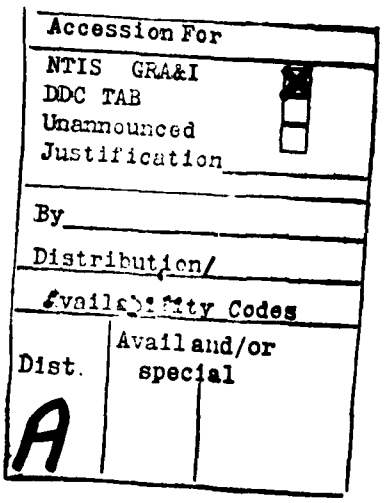
MISSION

The 1842 Electronics Engineering Group (EEG) has the mission to provide communications-electronics-meteorological (CEM) systems engineering and consultive engineering support for AFCC. In this respect, 1842 EEG responsibilities include: Developing engineering and installation standards for use in planning, programming, procuring, engineering, installing and testing CEM systems, facilities and equipment; performing systems engineering of CEM requirements that must operate as a system or in a system environment; operating a specialized Digital Network System Facility to analyze and evaluate new digital technology for application to the Defense Communications System (DCS) and other special purpose systems; operating a facility to prototype systems and equipment configurations to check out and validate engineering-installation standards and new installation techniques; providing consultive CEM engineering assistance to HQ AFCC, AFCC Areas, MAJCOMS, DOD and other government agencies.

DISCLAIMER

The use of trade names and specific equipment in this technical report does not constitute an official endorsement or approval of the use of such commercial hardware or software; this document may not be cited for advertising purposes.

AFCC TECHNICAL REPORT



FAULT-ISOLATION
IN
AIR FORCE BASE LEVEL DATA
NETWORKS

BASE TELEPROCESSING SYSTEMS
BASE COMMUNICATION SYSTEMS BRANCH
ELECTRONIC AND BASE SYSTEMS ENGINEERING DIVISION
1842 ELECTRONICS ENGINEERING GROUP (AFCC)
SCOTT AIR FORCE BASE, ILLINOIS 62225

10 SEPTEMBER 1980

REVIEW AND APPROVAL

Data contained in this report is current as of 1 August, 1980.

This report has been reviewed and is approved for publication and distribution.

Gerald T. Harris

GERALD T. HARRIS
Chief, Electronics Base
Systems Engineering Division

DATE 12 Sept 80

Robert W. Neill

ROBERT W. NEILL P.E.
Chief, Base Comm
Systems Branch

DATE 28 Aug 1980

Thomas H. Weaver

THOMAS H. WEAVER, JR.
TAM, Base Teleprocessing Systems

DATE 28 Aug. 1980

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER: 1842EEG/EEIC TR-80-7	2. GOVT ACCESSION NO.: AD-A090526
	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)*: AFCC Technical Report Fault-Isolation in Air Force Base Level Data Networks	5. TYPE OF REPORT & PERIOD COVERED: Final Report. 1 Oct 79 — 1 Sep 80
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): Thomas H. Weaver, Jr.	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS: 1842 Electronics Engineering Group, Base Communications Systems (EEIC), Scott AFB IL 62225	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: 66
11. CONTROLLING OFFICE NAME AND ADDRESS: Same as above.	12. REPORT DATE: 1 Sep 80
	13. NUMBER OF PAGES: 58
14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)*	15. SECURITY CLASS. *(of this report)*: Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Fault-Isolation
Data Networks
Data Transmission
Computer Networks

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

The objective is to provide a single-ended fault isolation capability for base level data networks which can be used by the senior level computer operator. The network is examined in terms of useful information which is inherently available. We then determine what information is required to isolate faults to the "which vendor" level, suggest means to extract that information and examine off-shelf devices to accomplish that extraction. Based on construction of a "Bare-Bones" fault isolation facility, we conclude that the objectives can be met with off-shelf devices and that the payback is between 2 and 3 years.

DD FORM 1 JAN 73 1473

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

1.0 INTRODUCTION.

Rapid advances in computer and computer communications technology, coupled with significant reduction in hardware costs, has led to increased useage of computer networks in both the private and public sectors; and once a computer network is acquired, the users become highly dependent on its successful operation. At the Air Force Base level, down-time in automatic data processing and automatic message distribution networks becomes a more serious problem as their complexity increases.

These base level networks range in complexity from a single computer with a few remote terminals to multiple computers with a large remote terminal population. As the network becomes more complex, the task of isolating failures also increases in complexity and this usually results in increased "down-time" per network failure.

1.1 Definition of the Problem.

Base-level networks generally consist of a central processing facility connected to a group of remote terminals. The terminal subsystem is usually in the form of a "tree" or "star" configuration and the connecting paths consist of on-base wire pairs, off-base voice channels, and combinations thereof. The terminal subsystem can consist of central processor hardware/software (communications controller), modems, conference bridges, digital hubs, time division and frequency division multiplexers, cryptographic equipment, and the remote terminal devices. In large terminal population networks, a data switch may be included, or a base telephone switch may be utilized.

It is this very profusion of devices with its associated maintenance responsibility split among the various vendors (some of which are government agencies) that is the basis of the problem to be examined. In a typical network, the following listed vendors could each be responsible for part of that network:

Central Processing Facility

- Processor hardware
- Operating system software
- Applications programs software

Communictions Facilities

- Modems
- On-base wire lines
- Off-base voice channels
- Crypto equipment
- Multiplexers
- Conference bridges
- Data switch hardware

Data switch software

Telephone switcher

Remote Terminal Facilities

Keyboard/video displays

Printers, and

Other terminal devices

In such a network, the operator has no means to determine which vendor has the problem when a failure occurs. As the network operator reports the problem to the various vendors, he usually faces a "finger pointing" exercise, with each vendor claiming that "the problem is on the other end". The effect of this exercise is to increase the network "down time" far beyond that actually necessary to locate and repair the failed element. One industry study indicates that two-thirds of the down-time is attributable to this problem. (1)

Within the DOD, historically, the technical control facility and associated maintenance patch and test facilities have provided fault-isolation capabilities for the long-haul networks. These facilities are present on both ends of any trunk/link and isolation procedures are a cooperative effort between the skilled technical controllers at the link ends. Most of the developmental work in the DOD has been directed toward improving this type of fault-isolation rather than toward a base-level capability which is significantly different.

This difference is significant for two basic reasons; i.e. the fault-isolation must be single-ended at the central computer facility, since test devices installed at each terminal location are not economically feasible; and the fault-isolation methods must permit successful operation by computer operator personnel, since it cannot be expected that full-time highly skilled technical controller positions can be justified for those relatively small and sometimes workday only scheduled operations.

To summarize, the objective is to provide a capability which will permit the computer system operator to rapidly determine, "Which vendor has the problem?"

1.2 Study Approach.

In order to isolate network problems, information regarding the status of each node and link in the network is required. Fortunately, these nodes and links, can provide such information as an inherent part of their operation. Section 2.0 discusses this aspect and reviews the kinds and sources of this available information. Section 3.0 analyzes the available information and determines the minimum amount required to meet the "which vendor do I call" fault-isolation objective. Section 4.0 proposes methods of extracting and utilizing the minimum required information, and Section 5.0 looks at off-shelf devices which accomplish this extraction and utilization. Section 6.0 proposes a "bare-bones" cost fault-isolation facility; Section 7.0 provides a cost and payback analysis for the "bare-bones" facility.

2.0 INFORMATION AVAILABLE IN THE NETWORK.

The information, which is inherently available in any computer communication network can be conveniently assigned to one of three domains; i.e. the data domain, the time domain, and the frequency domain. (2) These domains are divisions of the available information and cannot be precisely described by the electrical interface boundaries.

2.1 The Data Domain.

This domain is rich with information about the network. All network configurations will not, of course, contain all of the information discussed herein; examples of typical configurations will be given for those cases.

a. In all computer-to-terminal connections, the EIA standard RS-232C interface or the MIL STD 188-100 between the computer and the communications subsystem and between the remote terminal and the communications subsystem contain much of the data domain information (refer to Figures 2-1 and 2-2). First, it contains (on the data leads) all of the useful data being exchanged between the computer system and the remote terminal. If this user data is narrative in nature, the content itself provides information about the network; i.e. does it contain errors? Even if it is not narrative, it is in some prescribed format (columns, rows, groups, etc) and violations of the format can be observed. Another message format content which contains information is that in the message header and trailer. Depending on the coding used by the system, the header and trailer contain symbols such as: SOH (start-of-header), SOM (start of message), STX (start-of-text), ETX (end-of-text) and EOM (end-of-message). In some systems these symbols are sent as a unique single character code while in others, with a more limited code structure, they are sent as a unique sequence of alpha-numeric character codes. In either case, they have a specific format which can be observed for errors.

Another source of data domain information, available at the data lead interface, is the computer-to-terminal protocol; such protocol is only present when the terminal is under control of the central computer. This protocol can take many forms, but in general consists of either uniquely coded characters or uniquely grouped alpha/numeric sequences. This type of protocol usually provides for addressing a specific terminal, identifying a terminal which desires to send a message, and determining if a terminal or a specific terminal device is up and ready to receive a message. In most cases not only the content, but the sequence and timing between protocol events also provide useful information. In many networks, the computer polls (addresses) each terminal, in turn, which is connected to a multipoint channel. When a terminal recognizes its specific address, it answers the processor with an ACK (acknowledgment) or NAK (negative) and perhaps its station identifier. However, if the terminal does not respond within some specified time, the processor usually attempts to re-poll the terminal (maybe several times), and upon failure, alerts the system operator that the terminal is down because of communications. This, of course, may, or may not be true; the terminal may well be answering the poll, but too late.

The last source of data domain information available directly on the data leads is a pseudo-error rate which can be estimated by observing the number of parity errors in the received data stream.

b. With the EIA RS-232C interface (Figure 2-1) there are many options to accomplish, what has been dubbed, "modem handshaking" routines between the computer and the modem and between the terminal and the modem. As one example, a computer connected to an asynchronous half-duplex terminal (send and receive, but not simultaneously) might use the following handshaking routine:

(1) Both the computer and terminal have a logical one voltage level on the "data terminal ready" lead, indicating that the computer/terminal are up and ready.

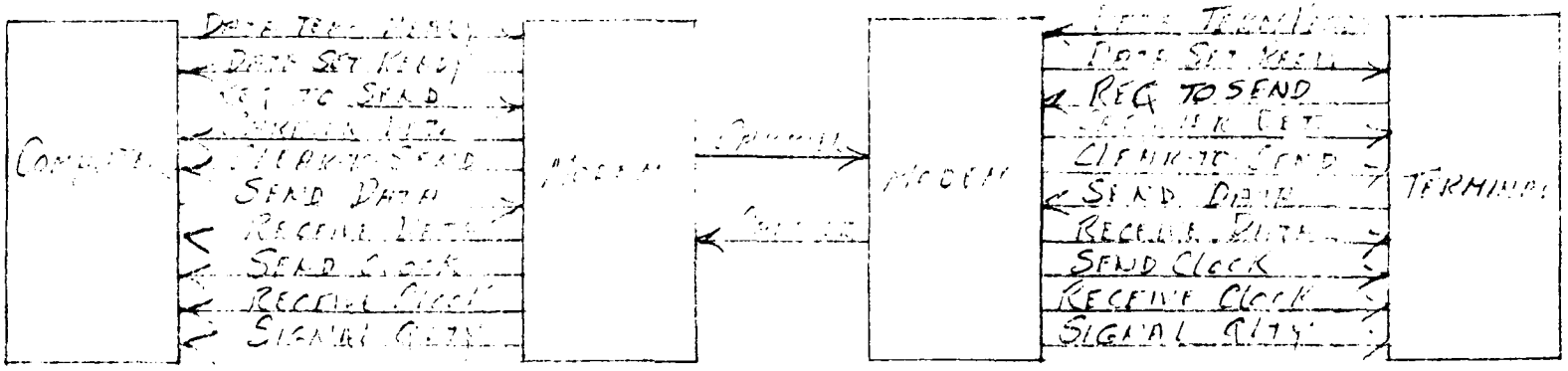


FIGURE 2-1 TYPICAL EIA RS-232C INTERFACE

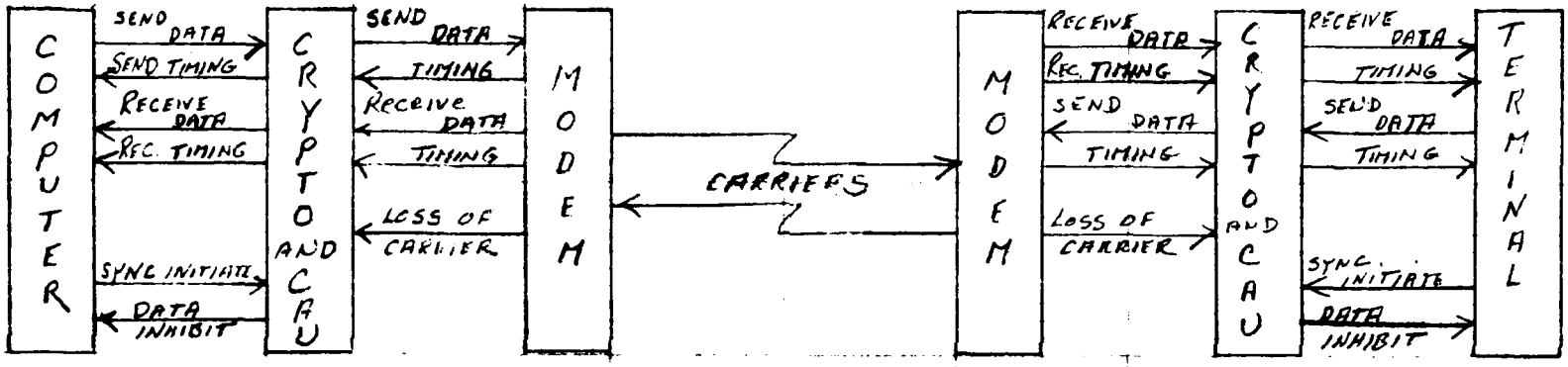


FIGURE 2-2 TYPICAL MIL STD 188-100 INTERFACE

(2) Both modems have a logical one voltage level on the "data set ready" lead, indicating that the modems are up and ready.

(3) The computer desires to send a message to the terminal; it places a logical one on the "request to send" lead, after checking for the logical one on the "data set ready" lead.

(4) Upon detection of the "one" on the "request to send" lead the modem at the computer end of the circuit turns on its carrier.

(5) Upon detection of the received carrier, the modem at the terminal end places a logical one on its carrier detect lead (if the terminal "data terminal ready" lead is at the logical one level) and turns on its carrier.

(6) Upon detection of the received carrier, the modem at the computer end places logical ones on its "carrier detect" and "clear to send" leads.

(7) The computer sends traffic to the terminal; upon completion it removes the logical one from its "request to send" lead which in turn causes the modem to turn off its carrier, and so on.

Not only can the sequence of events in the "modem handshaking" routine be observed and compared with the proper sequence to obtain status information, but the timing between each event can be observed for compliance with the established routine. In a manner similar to that described for terminal polling, each network has established time delays between, at least, some of the "modem handshaking" events; e.g. the time between placing the logic one on the "request to send" lead, and detecting a logic one on the "clear to send" lead. Delays beyond the maximum permitted by the network cause the event (if it occurs at all) to be deemed a failure; most networks make several attempts before alerting the system operation.

Even after a successful "handshaking" (during traffic flow), the logical state of these leads can be compared to the proper logic states as a source of information (that the connection to the terminal and the terminal are in order). In fact, in some networks, a specified set of constant logic states is the only information available; i.e. there is no "handshaking" routine. An example of this type would be a full-period, full-duplex synchronous channel in which all "handshaking" leads are always at the "one" level if the connected devices are up and running. A change from a one to a zero on any lead indicates a malfunction; e.g. a change to zero on the computer end modem "carrier detect" lead indicates loss of carrier from the terminal end modem. Examination at the terminal end might reveal a zero level on that modem "data set ready" lead, indicating a modem failure; or if coupled with a zero on the "data terminal ready" lead, indicating a terminal failure.

c. With the MIL STD 188-100 interface (with cryptographic equipment, including a CAU), there is no modem handshaking such as that with the EIA RS-232C interface. Most modern secure circuitry is operated in a full-period, full-duplex, synchronous or isochronous mode (even if the terminal is asynchronous half-duplex, it is converted to full-duplex synchronous or isochronous operation). The information available here is "steady-state" when the channel is up and running, and any change to that steady state indicates abnormal conditions. However, the indicators (Figure 2-2) are primarily concerned with the status of synchronization between the two crypto devices.

If the modem removes the logic one from its "carrier detect lead", or if the CAU detects a loss of crypto synchronization, the CAU changes the logic state on the "data inhibit" lead which blocks further transmission from the connected source (computer or terminal). The CAU then attempts to re-synchronize the cryptos (several times); if

successful, data transmission is resumed, and if not successful, out of sync alarms are activated. The computer or terminal, based on parity error content, or the absence of the received data stream, can initiate the CAU re-synchronization process by changing the logic state on the "sync initiated" lead.

d. Following is a summary of the "data domain" information that is inherently available in the network;

On-Data Leads

Narrative message error content
Message format error content
Message header/trailer error content
Computer-to-terminal protocol
    Content
    Timing
Computer-to-terminal parity errors

RS-232C Handshaking Leads

Sequence of change of lead status
Timing of change of lead status
Change from steady-state lead status

MIL STD 188-100 Control Leads

Change from steady state lead status

2.2 The Time Domain.

Except for failure or circuitry within the connected devices (processor, multiplex, crypto, modem, terminal), anomalies in time domain information are a reflection of anomalies in the frequency domain (discussed below). None-the-less, the time domain information is very useful toward detecting network faults.

a. On asynchronous circuits, all time domain information is available on the send and receive data leads. On the send data lead we can observe the data bits as they are released by the processor/terminal. Depending on the character code structure used and the bit rate, each character will consist of a series of bits, each of which has a specific bit length (in terms of time); e.g. in an ASCII coded sequence each character may consist of a start bit, 7 information bits, and a parity bit, all of which are one bit time in length, followed by a stop pulse which may be of a different length (common lengths are 1.0 and 2.0 bit times). Comparison of the transmitted character structure and individual bit lengths versus the theoretically perfect bit structure provides information about the performance of the transmitting device.

On the receive data lead we can observe and compare the same bit structure, but network status content is considerably greater; i.e. any defect in the bit structure is an indication of the condition of the entire transmitter-to-receiver path. These path conditions, and the resulting bit defects, may be divided into two groups; steady-state and variable. All of the path conditions produce defects (distortion) in the bit time relationship; however, the steady-state distortion is always present while the variable conditions produce changing distortion which is added to the steady-state distortion value. Thus, discrete changes in the steady-state distortion as well as the presence of varying distortion in the receive digital stream can be used to detect path problems.

b. On synchronous circuits, time domain information is available on the send/receive data leads and on the send/receive clock leads. Most base-level network synchronous circuits operate in the following manner; the modems contain an accurate crystal oscillator which drives a count-down chain to provide a digital data clock stream. This stream consists of alternating ones and zeros at twice the desired channel bit rate and is commonly called a "2X data clock". The 2X clock is provided from the modem to all of the transmitting devices (processor/terminal, multiplex, crypto and the transmit modem circuitry) on the send timing lead. All data appearing on the send data lead is released under control of this 2X lock with each bit of the same length. Each modem transmitter thus acts as the master clock for one direction of transmission with the distant modem receiver acting as a slave to the master clock. The modem receiver accomplishes this slaving by recovering timing information from the received data stream; i.e. the 2X clock stream is not transmitted independently over the transmission path. Circuitry in the modem receiver accomplishes this timing recovery by observing the average time between bit transitions on the data stream over a specified period of time. Differences between this average recovered timing information are then used to correct internal modem receive 2X clock circuitry (independent of the transmit 2X clock circuitry); this corrected 2X receive clock stream is provided both to connected devices and used to clock the data stream from the modem on the receive data lead. Data bits which have been distorted by the transmission path are thus regenerated by the modem receiver (retimed) and comparison of the receive data bit timing tells us little about conditions on the transmission path; it does, however, tell us whether or not the modem receive timing recovery circuitry is working properly or that this circuitry has lost synchronization due to extreme degradation on the path (an alarm is normally provided in this case). Comparison of the transmit clock rate against some standard clock provides us with information about the accuracy and stability of the modem transmit clock. Comparison of the relationship between the bit transition on the data leads and the clock transitions on the associated clock leads of each connected device provides information regarding input/output circuitry; there is normally some small amount of skew permitted by the applicable standards. Observation of the 2X clock on the receive timing lead and of the data on the receive data lead will reveal a jittering of the pulse edges (clock jitter); this is caused both by the timing recovery circuitry making altenuate plus and minus clock corrections and a phase jitter component (in the frequency domain) of the received signal from the transmission path.

c. Following is a summary of the "time domain" information that is inherently available in the network;

On Data Leads

Digital pulse time distortion
Digital pulse jitter

On Clock Leads

Data clock rate
Data clock presence/absence
Data clock pulse jitter

Comparison of Data/Clock Leads

Skew between pulse edges

Other

Out of sync indicators

2.3 The Frequency Domain.

The modems shown in Figures 2-1 and 2-2 convert the data signals to a form suitable for the transmission path and reverse the process at the distant end. These modems fall into two general classes; i.e. those designed to transfer the data signal over a voice channel having a nominal bandwidth of 4 KHz (due to the filters contained in the telephone voice channel multiplex hierarchy) and those designed to transfer the data signal over wire paths which are not constrained by a 4 Hz bandwidth limitation. All of the voice channel modems utilize the data stream to modulate/demodulate an analog audio frequency carrier or carriers in amplitude, frequency, phase or combinations thereof. Wire path modems (short-haul modems) can operate in either of two modes; i.e. modulate/demodulate an analog audio frequency carrier, or modulate/demodulate a digital carrier. With the former, the transmitted signal is quasi-analog in nature, while with the latter the transmitted signal is digital baseband in nature. Each modem is designed to provide a specified grade-of-service (maximum bit-error rate) over a transmission path whose parameters meet a specified set of values.

a. Steady-state parameters. These specified parameters are those which are expected to remain relatively fixed in value once the transmission path is established. Changes in the values of these parameters indicate that the path has been changed in some manner.

(1) End-to-end attenuation. This is usually stated in terms of the attenuation at 1000 Hz from the transmitter output to the input to the receiver. Most modem transmit levels are set below Odb to prevent interference to other cable pairs in the same cable or other voice channels in the multiplex group. Most modem receivers have a receive signal level (RSL) dynamic range of about 30 db (0 to -30 db) and thus a path having as much as 20 db end-to-end attenuation could be expected to provide good service with a 10 db margin; i.e. if the signal-to-noise ratio (SNR) is adequate.

(2) Background noise: This (also called idle channel noise) consists of noise from many sources and is usualy lumped into a single value; these sources include the thermionic noise generated within each electrical device (including wire) in the path, noise induced into the path from external sources (including adjacent paths). The total value of all of this noise has been shown to have a density function which is gaussian and a frequency content which is flat over the band (called "white noise"). This differentiates this noise from impulsive noise which is neither gaussian nor white. Each modem receiver is designed to make proper logical decisions (within a specified error probability) at a specified signal-to-noise ratio. A common modem may perform at a bit error rate (BER) of 1×10^{-7} at an SNR of 20 db, at 1×10^{-6} at an SNR of 15 db, and at 1×10^{-5} at an SNR of 12 db, etc. Thus, the received signal level must be considered in conjunction with the background noise; i.e.

$$\text{SNR} = \frac{\text{Sig Level db.}}{\text{Noise level db (background)}}$$

(3) Frequency response, and envelope delay. Modems are designed to transfer data at some specified bit rate over a path having some specified useful bandwidth. This bandwidth is usually specified in terms of amplitude and phase distortion of the received signal at specific frequencies (or bands of frequencies) as compared to the amplitude and phase of the received signal at a reference frequency (usually 1000 or 1200 Hz). As the modem signal is propagated along the transmission path, the frequency components of the signal are not affected equally; i.e. some frequencies are attenuated more or less than others and some frequencies are propagated faster or slower than others. If the difference in attenuation and propagation time were a linear function of the frequency, modem design would be significantly more simple; however, they are not

linear functions, hence the term distortion is used to describe the non-linearity of these functions. These distortions in amplitude and phase cause smearing of the signal pulses which in turn causes overlap of adjacent pulses (intersymbol interference). Depending on the severity of the intersymbol interference and the polarity of adjacent pulses, the receiver may make incorrect logical decisions - bit errors. In the end result, the receiver decision making circuitry sees this distortion as noise - in addition to the idle channel or background noise.

(4) Frequency offset and phase jitter. Radio and cable transmission paths which utilize voice channel multiplex, up/down converters or other devices which change the frequency band occupied by a data signal, do not always restore the data signal frequency band (at the receiver) exactly as it was originally transmitted; i.e. a data signal occupying the 500 to 2500 Hz band with its carrier at 1500 Hz might be received as a signal occupying a 510 to 2510 band with its carrier at 1510 Hz. Most modems designed for 4 KHz voice channel use will perform adequately with a frequency offset of $\pm$5 Hz. Phase jitter is another form of signal degradation inherent in the voice channel network and has been found to be predominent at the primary power frequencies and harmonics thereof; i.e. the phase variations in the signal are a result of direct frequency and phase modulation of the signal through primary power sources. Again, the end result in the receiver decision making circuitry is additional noise.

(5) Impuse Noise. By definition, impulse noise is not steady-state, i.e. there is either a noise pulse present or there is not. However, it is included here since on data paths which traverse the telephone system cable plant, a relatively constant quantity per unit time of noise impulses are induced into the path by the electro-mechanical telephone switching machine. It is relatively consistent, not as a continuous level of noise, but as the number of impulses above some threshold over a specified period of time. The impact of impulse noise, above the modem receiver designed threshold, is to cause bursts of errors rather than the randomly distributed errors caused by the other steady-state parameters.

b. Variable parameters. Changes in the value of any of the steady-state parameters, of course, indicate that some change in the transmission path has occurred; these changed values usually remain at the new value until some action is taken to restore them to their previous proper values. Here, variable means those changes in parameter values which are short-term in nature with the old valves being restored without any action on the part of system operators. These variations can be caused by actions of operator and maintenance personnel, severe fading and multipath on radio paths, by externally induced signals, and noise (CB radio's, automobile ignition, etc), fluctuations in primary power sources, and the effects of lightning. The end result of these variable parameters is to increase the total noise in the receiver decision circuitry, thus increasing errors.

(1) Dropouts. Sudden short-term loss of the signal.

(2) Amplitude Hits. Sudden short-term increases in the signal level.

(3) Phase-hits. Sudden short-term dispersions in the phase relationships of the signal.

(4) Interference. Sudden short-term presence of an external signal at a level sufficient to cause errors.

(5) Impulse Noise. Sudden short-term noise bursts significantly above the normal impulse noise levels or occurring more often than normal.

c. All of the information about the frequency domain is, of course, reflected in the information available in the data and time domains (error rate, pulse jitter, timing skew, loss of synchronization, etc). Direct information regarding the frequency domain is only present on the transmission path side (line side) of the modem, except for one EIA RS-232C and one MIL STD 188-100 interface lead (carrier detect) which merely indicates the presence or absence of the receive signal. On the send line-side, the information is primarily that regarding the characteristics of the signal as it enters the transmission path; e.g. level, power spectrum, frequency. On the receive line-side information about all of the frequency domain parameters is available, but more difficult to observe than data and time domain information.

One might be tempted to advocate ignoring the frequency domain information since the end result of all degradation in these parameters is an increase in the total noise as seen by the receive decision making circuitry, which in turn, results in an increase in error rate which is observable in the data domain. However, observation of the error rate does not determine what caused the change in the rate, it only determines that it has changed.

d. Summary of Frequency Domain Information

Steady-State

Received signal level (RSL)
Idle channel noise
Signal-to-noise ratio (SNR)
Frequency response
Envelope delay
Frequency offset
Phase jitter
Impulse noise (normal)

Variable (Sudden Short-Term)

Signal dropouts
Amplitude hits
Phase hits
Interference
Impulse noise (abnormal)

3.0 MINIMUM INFORMATION REQUIRED.

As previously discussed, the objective is to provide a capability which will permit the system operator to determine which vendor has the problem and the network information provided to the system operator should not be more than is required to meet that objective. The operator does not need to determine what the specific problem is within the processor, terminal or transmission path, but only that the problem is within some specific vendor's area of responsibility. Use of a system block diagram lends itself to this approach; Figures 2-1 and 2-2 will be utilized for the following discussion regarding the minimum information required. While specific networks will differ from these examples the differences will be in details which will not significantly change the approach discussed herein. We will approach the determination of what information is required by isolating faults.

3.1 An Asynchronous Network. Normally, the first indication that a problem exists comes from either the computer operator (who reports that such and such a terminal is out because of communications) or from the terminal operator (who reports that the computer system is down). Either report may be correct, or incorrect; but even if correct needs to be further identified as to which vendor is responsible. The first step in this direction is, of course, to more completely define the problem; i.e. does the terminal/computer respond at all, does the response contain errors, etc?

a. Modem Handshaking. Assuming that the network uses a modem handshaking routine (as described in paragraph 2.1b above) it must first be determined if this routine can be successfully accomplished. By having the computer operator call up the routine on the desired channel, the sequence and timing of the change in status of those control leads can be observed. In addition, the actual voltage level must be observed since EIA RS-232C specifies that the logical voltage must exceed +3 volts or -3 volts. The following sub-paragraphs are keyed to Figure 3-1.

(1) Prior to the start of the handshaking, the data terminal ready lead (at the processor-end) and the data set ready lead (modem) should be at the logical one level (above +3V). If either is not at this level, the problem is obviously in the processor or modem. The logical one indicates the device is powered-up and on-line. Other than a logical one indicates the opposite condition.

(2) The first lead involved in the routine is the request-to-send which should change from a logical zero to a logical one level. If it does not, the problem is in the processor.

(3) If the request-to-send lead does change to a logical one, the clear-to-send lead should change to a logical one within the establisheh "time-out" period.

(4) If the clear-to-send lead does not change to a logical one, then observe if the carrier-detect lead changes to a logical one. If it does, the problem is in the modem.

(5) If the carrier detect lead does not change to a logical one, then observe (on the signal line side of the modem) if the modem send carrier is present at the proper output level. If it is not, the problem is in the modem.

(6) If the send carrier is present and at the proper level, then observe if the receive carrier is present at the proper level. If it is, then the problem is in the modem.

(7) If the carrier is not present at the proper level, then the problem could be in the distant terminal, distant modem, or in the transmission path (either direction).

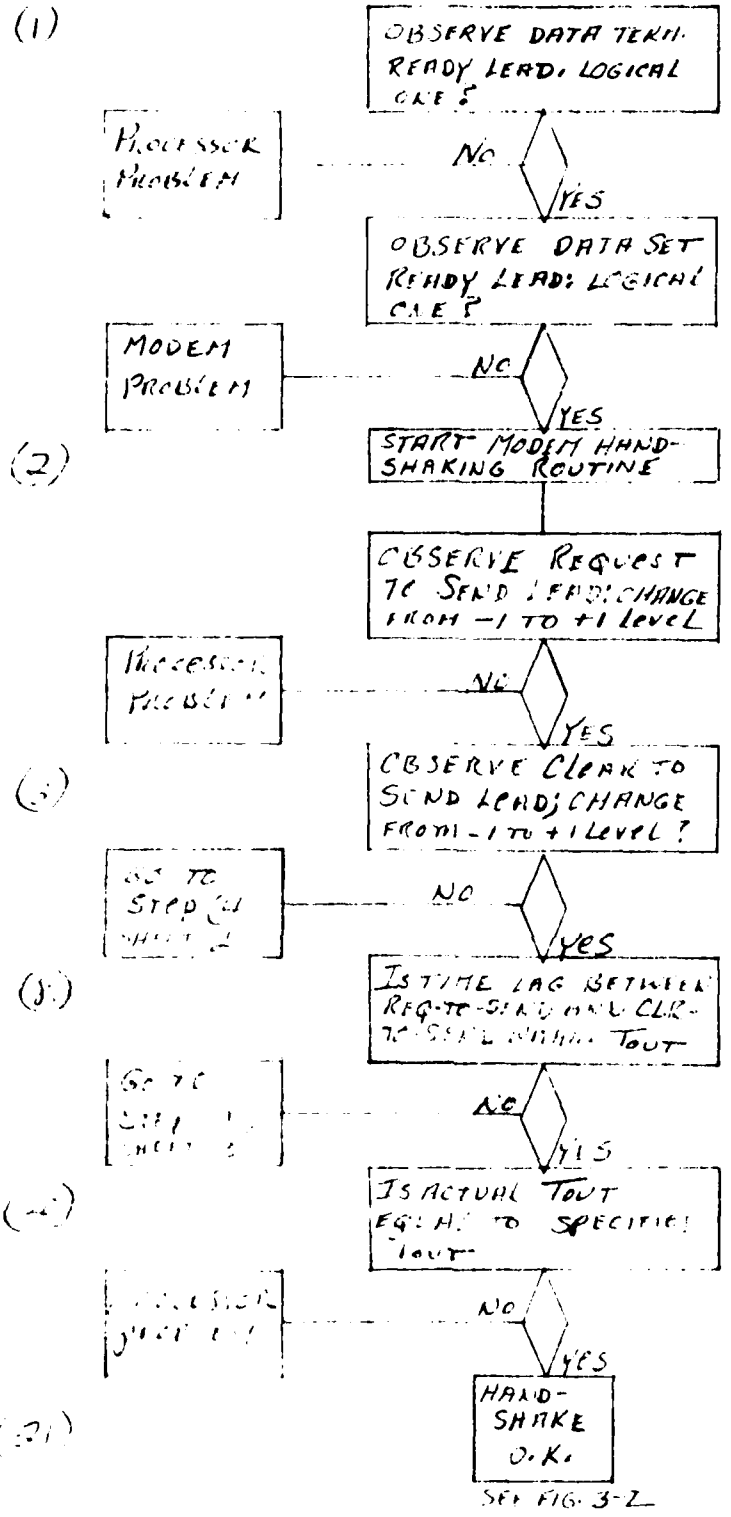


Figure 3-1 Communication Input Isolation RS-232C Asynchronous Network Modem Handshake

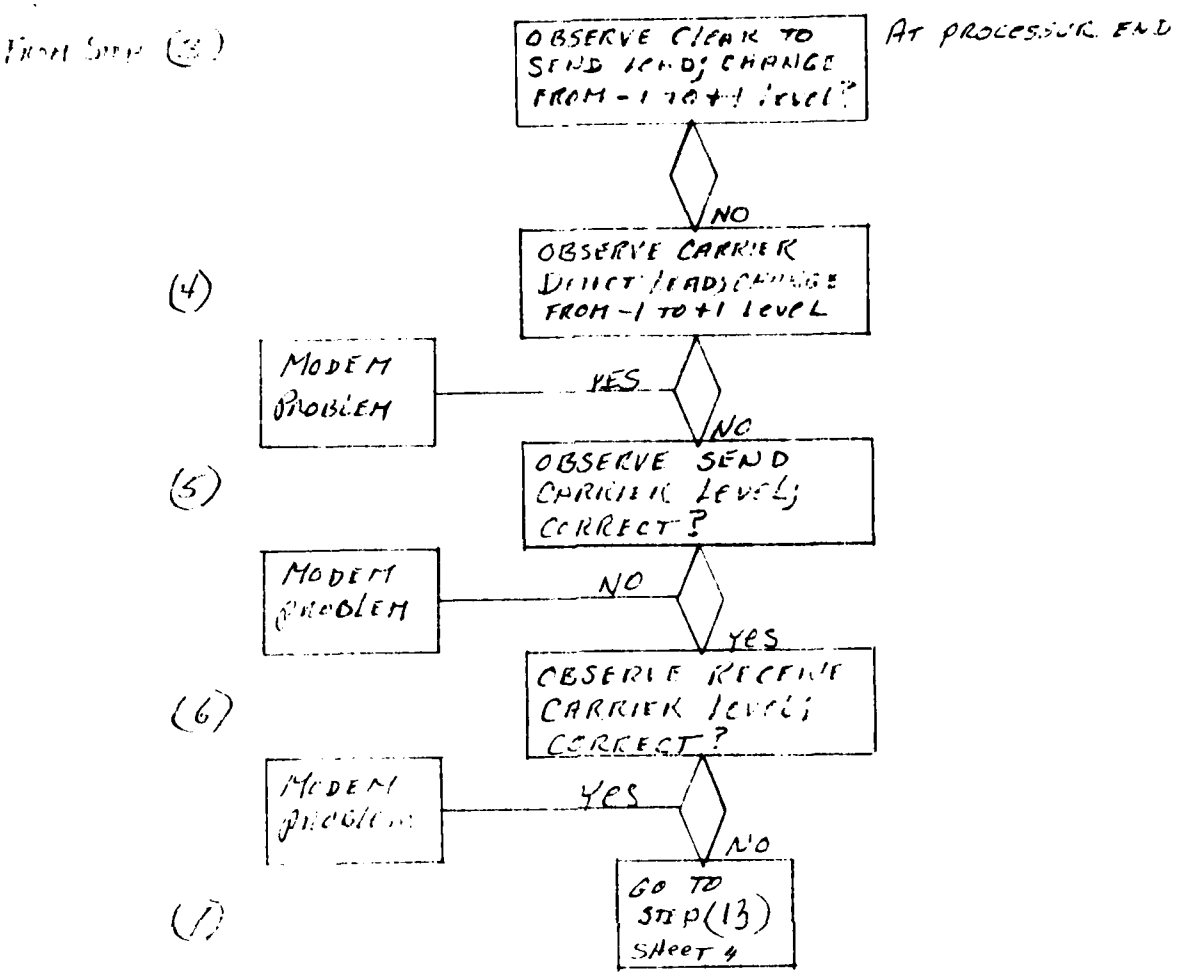


FIGURE 3-1 (SHEET 2 OF 4)

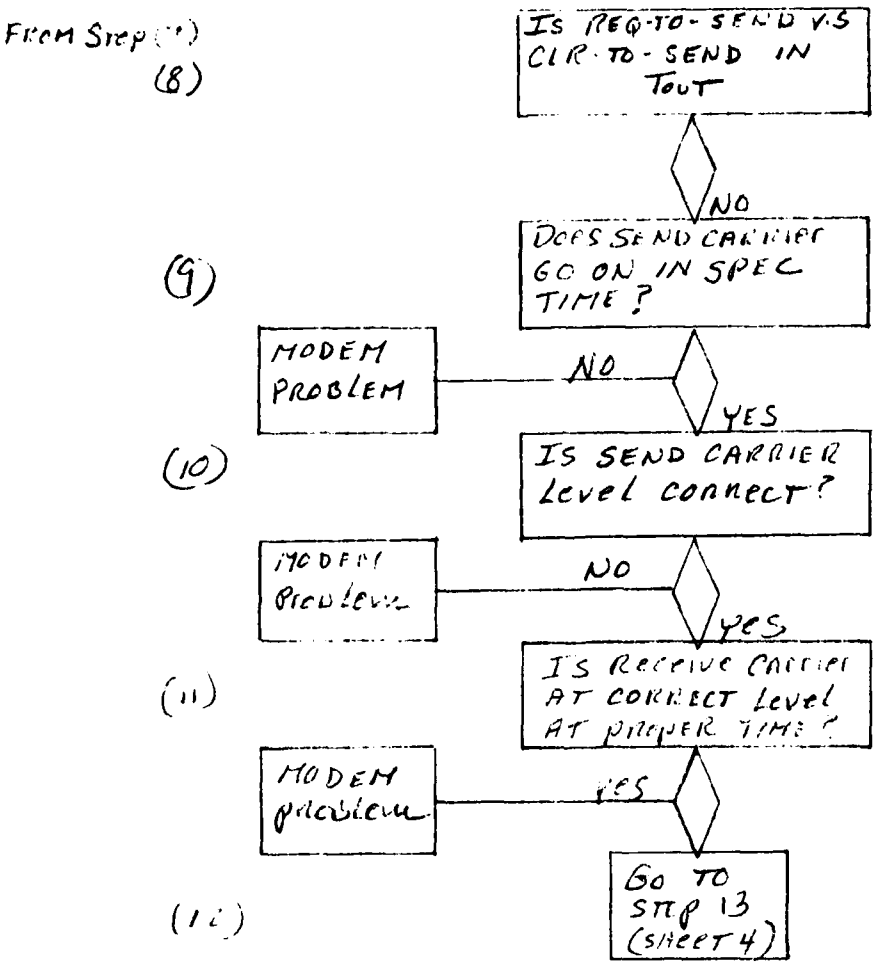


FIGURE 3-1 (SHEET 3 OF 4)

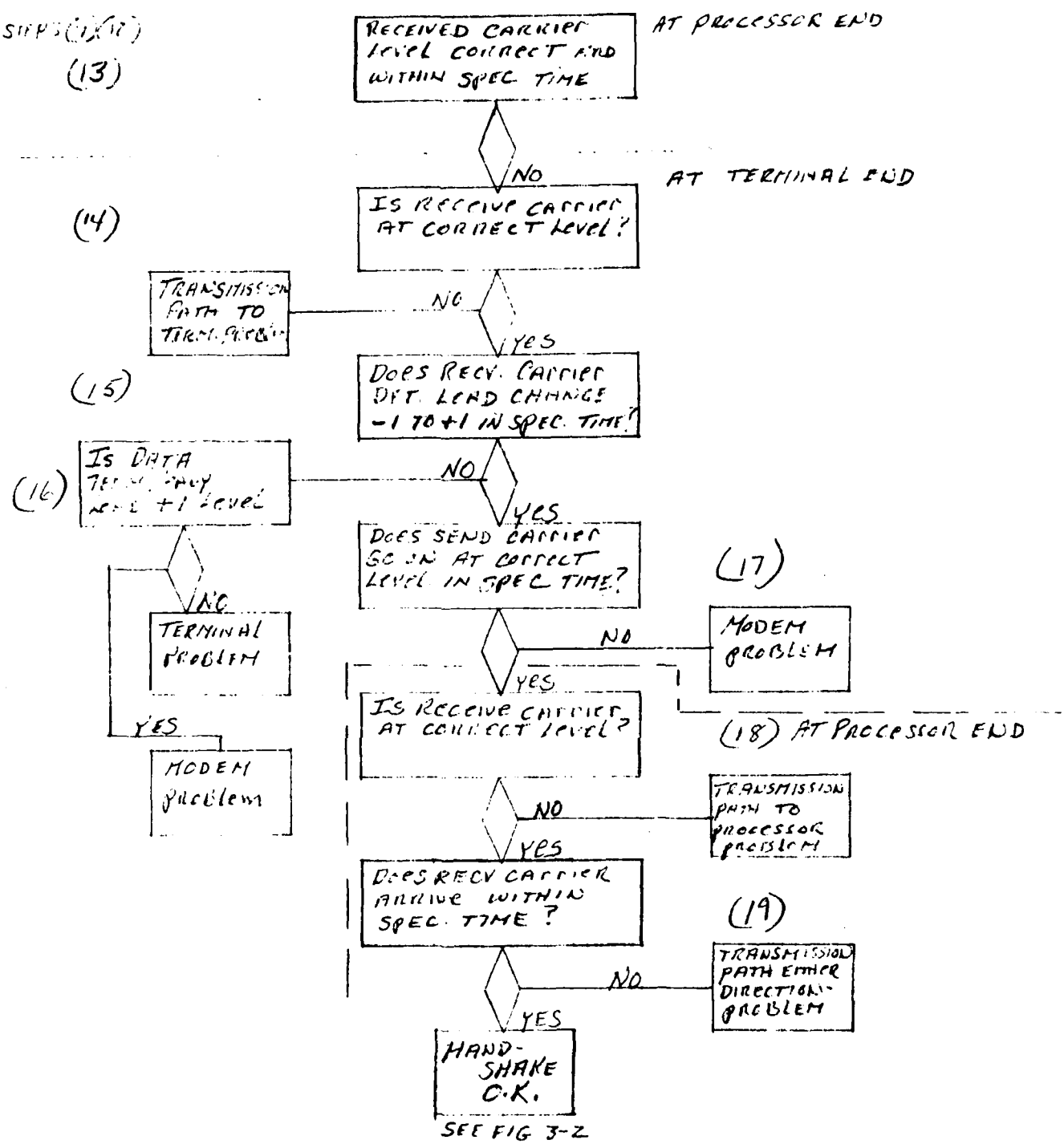


FIGURE 3-1 (SHEET 4 OF 4)

(8) Returning to the decision point a step (3), if the clear-to-send lead does change to a logical one, observe if the time between the change of the request-to-send lead and the change of the clear-to-send lead is within the established time-out period.

(9) If the above time exceeds the time-out period, observe if the modem send carrier goes on within the specified time after the request-to-send lead goes to a logical one. If it does not, the problem is in the modem.

(10) If the send carrier goes on within the proper time, is it at the proper level? If it is not, the problem is in the modem.

(11) If the send carrier is at the proper level, observe if the received carrier is received within the proper time and is at the proper level. If it is present at the proper level and time, the problem is in the modem.

(12) If the carrier is not present at the proper level or within the proper time, then the problem could be in the distant terminal, distant modem, or the transmission path (either direction). This brings us to the same decision point as was reached in step (7).

(13) When we reached step (7) and step (12), we had determined that the processor and its modem were on-line, the processor had placed a logical one on the request-to-send lead, the processor-end modem had turned its send carrier on within the proper time period and that the send carrier was at the proper level. We had also determined that the processor-end carrier detect lead did not change to a logical one level because the carrier received at the processor-end was either not present, not at the proper signal level, or did not arrive within the proper time period.

(14) To proceed further, information at the terminal-end is now required. Observe if the carrier as received at the terminal is present at the proper level. If it is not, the problem is in the processor-to-terminal direction in the transmission path.

(15) If the carrier is present at the proper level, did the carrier detect lead change to a logical one within the required time period (from presense of carrier to change in lead status).

(16) If the carrier detect lead does not change to a logical one the problem is in the terminal if the data terminal ready lead is not at the logical one level, or it is in the modem if the data terminal ready lead is at the logical one level. If the carrier detect lead does change to a logical one, but not within the required time period, the problem is in the modem.

(17) If the terminal-end carrier detect lead does change to a logical one within the proper time frame, next observe if the terminal-end modem places its send carrier on the line at the proper level within the proper time frame. If it does not, the problem is in the modem.

(18) If the terminal-end modem does place a proper level carrier on line, but the processor-end does not receive a carrier or does receive a carrier with an improper level, the problem is in the terminal-to-processor direction in the transmission path.

(19) However, if the processor-end does receive a proper level carrier but not within the specified time period, the problem could be excessive propagation delay in either or both directions of the transmission path. This frequently happens in long-haul paths when the common carrier alternate routes the path for maintenance purposes; it should not occur within on-base wire paths unless one route contains multiplexing devices (which add serial delay) and the other route does not.

(20) Now, return to step (9) at which point it had been determined that the processor had placed a logical one on the request-to-send lead and the processor-end modem had placed a logical one on the clear-to-send lead within the established time period. Next observe if the actual processor time-out period is the same as the specified time-out period (time between processor placing logical one on request-to-send lead and removing it). If the processor time-out is shorter than that specified, the problem is in the processor.

(21) If the processor time-out period is correct, the hand-shaking routine is successful and the reason for the computer operator reporting that the terminal is out to communications must be found elsewhere.

b. Processor-to-Terminal Protocol. As previously discussed, the information available within this protocol consists of errors in content, format and timing. In the fault-isolation decision tree (Figure 3-1), it was determined that if the modem handshaking routine was successful, further information was required to determine why the computer operator had the terminal logged out to "Communications". The next step is to observe the computer-to-terminal protocol as presented on the data leads. The following paragraphs are keyed to Figure 3-2.

(1) In our example, it is assumed that the processor first sends out a query to the terminal in a specific format; it contains an alerting character string (so the terminal knows a query is coming), the terminal address (several numbrs), a query message consisting of several character sequences in a specific order (are you ready to receive traffic, is your card punch on?), and an end-of-query character string. The processor query can be observed on the send data lead at the processor. Are there any errors in the format, in the content, in the characte" parity? If the answer to any of these questions is yes, the problem is in the processor.

(2) If the outgoing query is error free, then observe the terminal response on the receive data lead at the processor. Does the terminal respond at all? If not, the problem could be in the distant terminal, modems or the transition path.

(3) If the remote terminal does respond, observe if the response is proper (format and content). If not, the problem is in the terminal.

(4) If the terminal response is proper, does it contain parity errors?

(5) If the response does not contain parity errors, was it received within the designated time-out period? If it was received on time, then either the protocol routine was successful or the problem is in the processor. If it was not received on time, the problem is in the distant terminal.

(6) Going back to step (4), if the terminal response does contain parity errors, observe the send data lead at the terminal-end. Did the response leave the terminal free of errors? If not, the problem is in the distant terminal. If it left free of errors, then the trouble could be in the modems or the transmission path.

(7) Going back to step (2), if there is no response from the terminal as observed on the receive data lead at the procession, observe the receive data lead at the terminal. Was the query received and without errors? If yes, the problem is in the terminal. If not, the problem could be in the modems or transmission path.

(8) At step (7) the situation existed that the processor had transmitted a query without errors, but the query either was not received, or received with parity errors by the terminal. At step (6) the situation was similar; the terminal had transmitted a response without error, but it was received by the processor with parity errors. In each

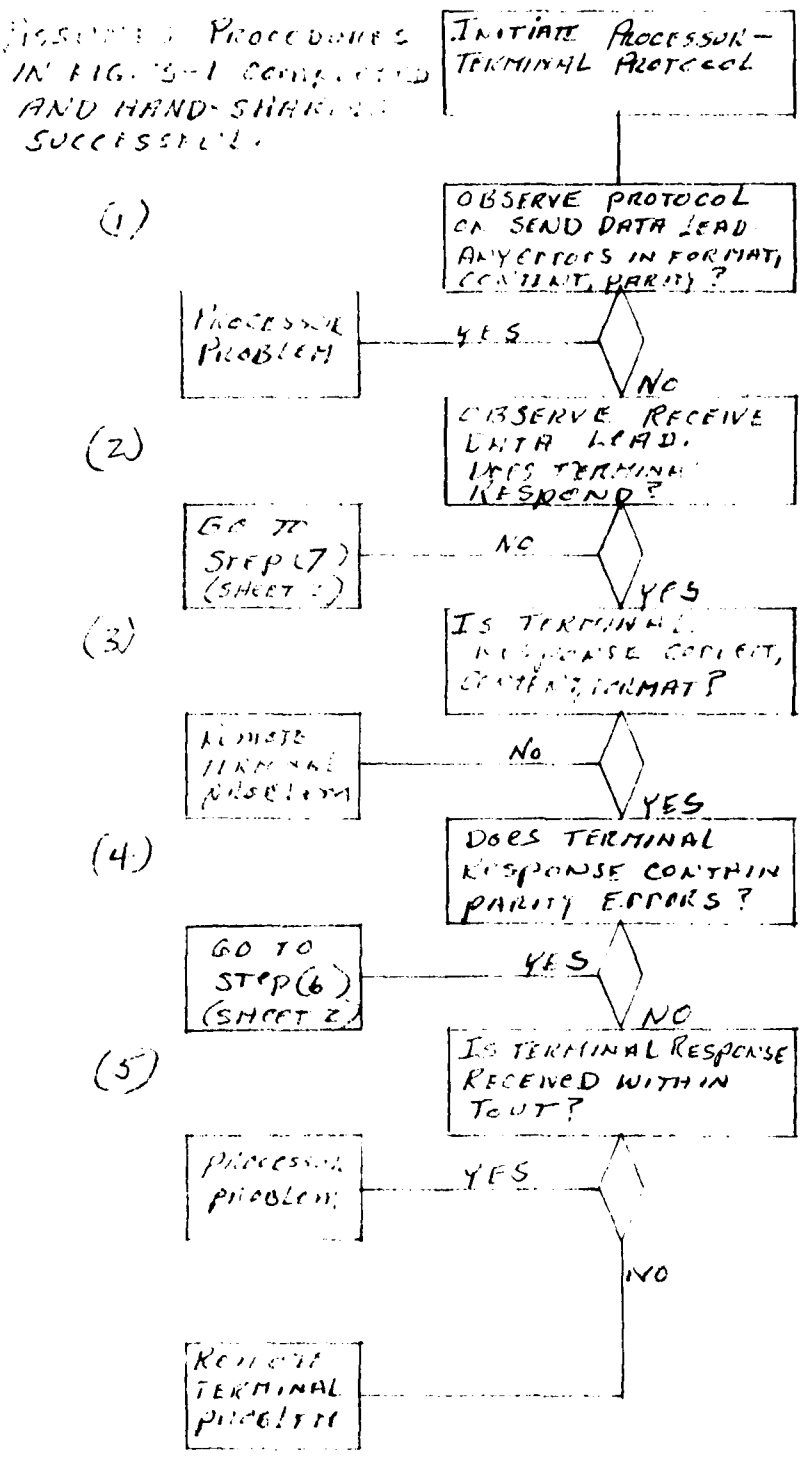


FIGURE 3-2 FAULT ISOLATION RS 232C.
(SHEET 1 OF 3) ASYNCHRONOUS NETWORK PROCESSOR-TO-TERMINAL PROTOCOL

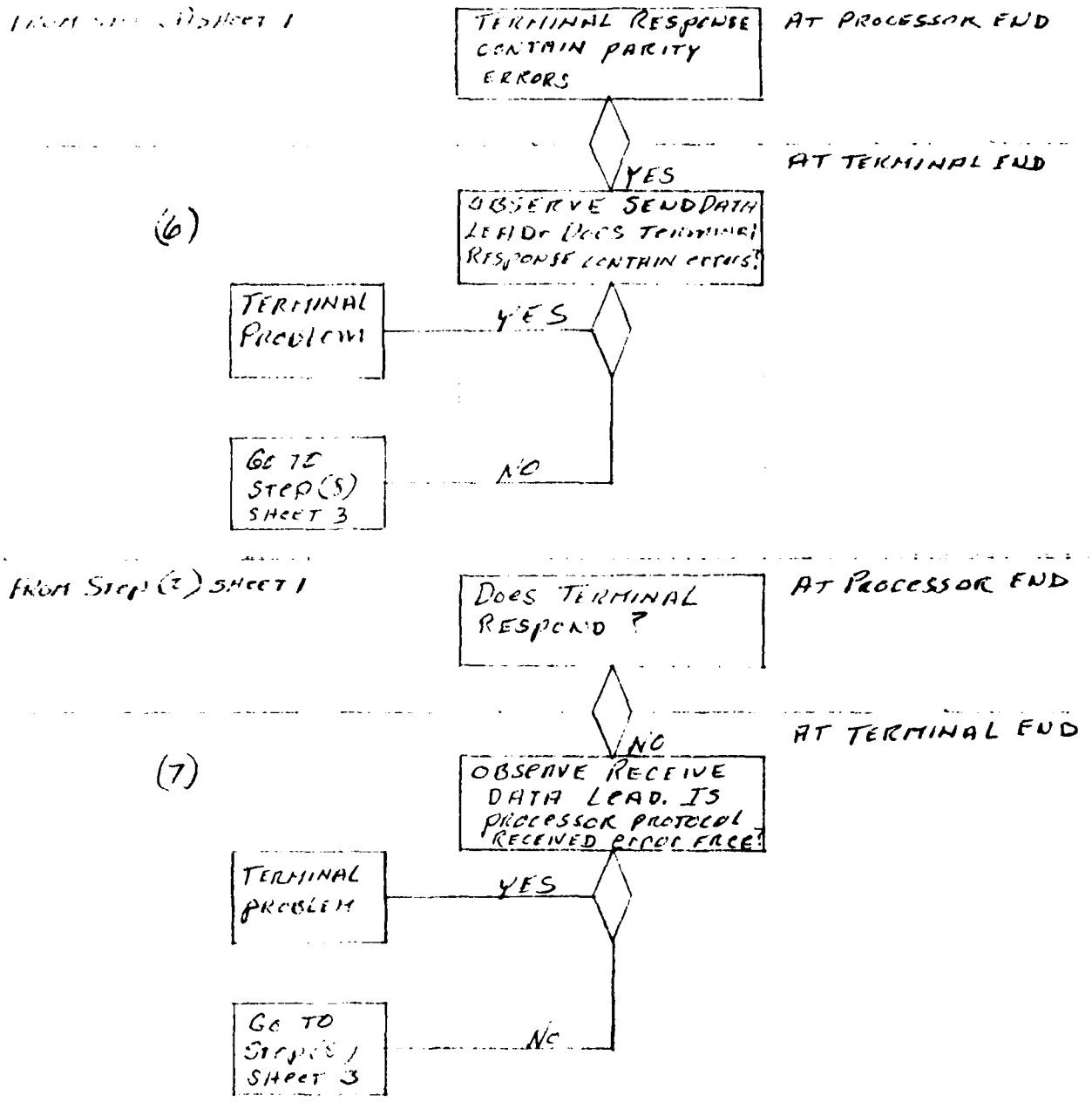


FIGURE 3-2 (SHEET 2 OF 3)

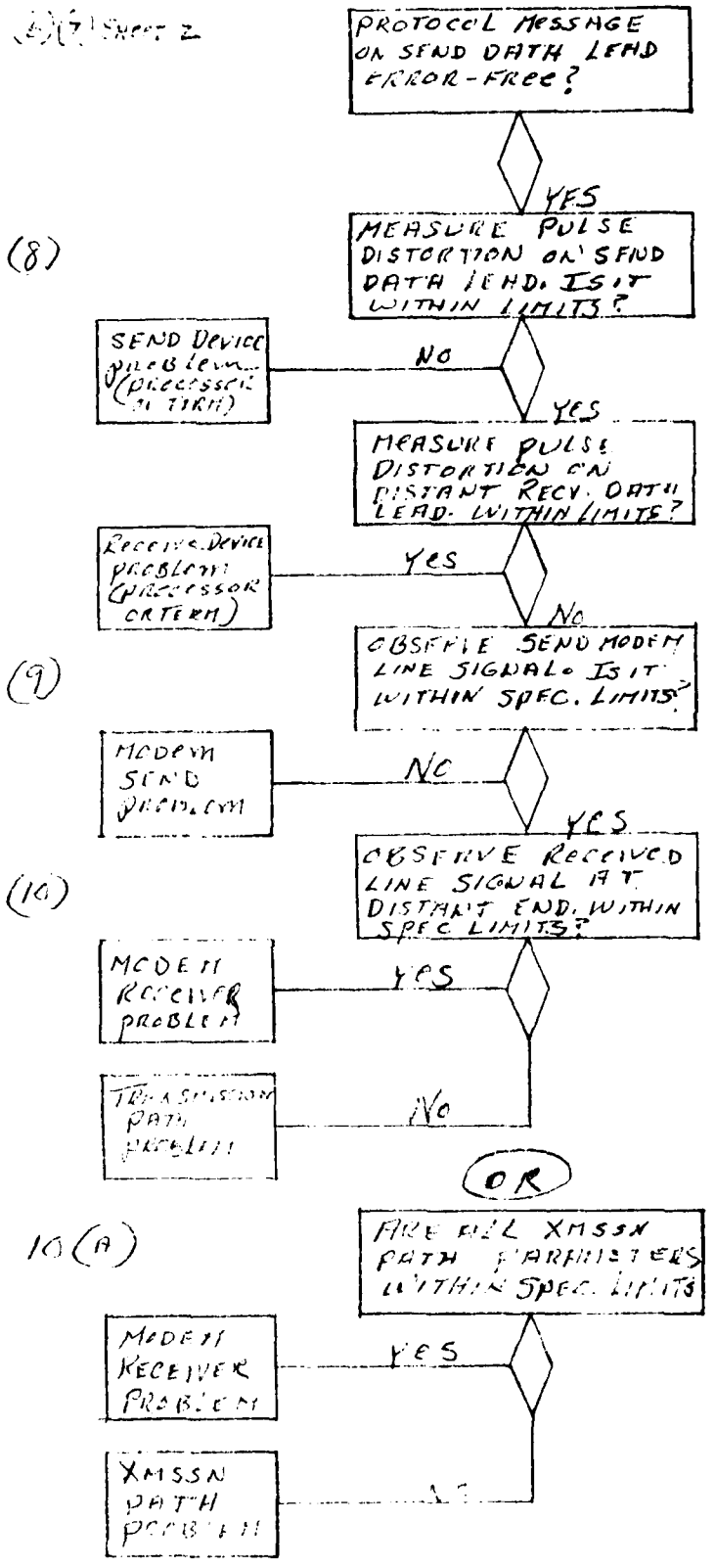


FIGURE 3-2 (SHEET 3 OF 3)

case we stated that the problem could be in the modems or transmission path. Actually the problem could also be in the transmitting line driver in the processor or terminal; i.e. although the transmitted bit stream does not contain errors, the pulses may be distorted to such an extent that when added to the normal pulse distortion caused by the transmission path, that the modem receiver makes erroneous bit decisions. The trouble could also be in the receiver in the processor or terminal; i.e. the received signal pulse distortion is within the limits of the receiver decision making circuitry, but that circuitry is making errors. If we measure the pulse distortion or the send data lead and it is not within specified limits, the problem is in the send device driver (processor/terminal). If the send pulse distortion is within limits, and measurement of the pulse distortion as the distant end receive data lead shows that the distortion is within limits, the problem is in the receive device (processor/terminal) receiver.

(9) If the sending pulse distortion is within limits, but the receive distortion exceeds the limits, the problem could be in the modems or transmission path. The next step would be to determine if the quasi-analog signal transmitted by the sending modem is within tolerances. Although this information is available at the modem/transmission path interface, it is difficult to measure (requiring complex test instrumentation; in Section 4.0 we will discuss methods to extract all required information or when such extraction is too difficult, methods of obtaining related information). However, at this point, assume that the required information regarding the quality of the transmitted (and received) modem quasi-analog signals can be obtained. If the transmitted signal quality is not within limits, the problem is in the sending modem.

(10) If the sending modem signal is correct and that signal is received at the distant end correctly, then the problem is in the receiving modem. If the received signal is not within tolerance, the problem is in the transmission path.

(10)(a) Alternately, instead of measuring the quality of the received quasi-analog signal, we could measure all of the transmission path parameters to determine the path quality and thus isolate the problem. Measurement of those parameters is also difficult and alternate methods will be discussed in Section 4.0.

c. Message traffic. In step (5) of Figure 3-2, it was determined that either the computer-to-terminal protocol was successfully completed, or the problem was in the processor and we proceeded on the latter determination. What if the protocol was successfully completed, but the computer operator still insisted that the terminal was out due to communications.

(1) Most systems employ a parity error detection scheme and a procedure for automatic request for re-transmission (ARQ) of messages (or data blocks) received containing errors. Most systems also limit the number of ARQ's and if the message or data block cannot be received without errors within the limit (usually two or three times), the channel is logged out.

(2) The bit errors which cause the parity errors can be divided into three groups based on their occurrence patterns.

(a) Regular occurrence; in this case, the bit error is always in the same bit position in each character, always in the same character, always in the first character in each block, always in the shift-function character, etc. This type of error is predominently a function of the transmitting device (processor/terminal) if the errors are contained in the transmitted signal. The problem would be in the receiving device if the signal was being transmitted and received without error, but interpreted erroneously by the receive device (printer, etc).

(b) Random occurrence; in this case, there is no pattern to the distribution of bit-errors and the information available consists of the average bit-error-rate (BER). If the BER is above the normal for the channel, we would proceed to isolate the problem via manner similar to that used in Figure 3-2 for parity errors in the computer-to-terminal protocol.

(c) Bursty occurrence; in this case, the errors have neither a regular pattern nor a random distribution; instead they occur in groups of bits. This type of error problem is predominantly caused by impulse noise on the transmission path which can be measured.

3.2 A Synchronous RS-232C Network. In synchronous networks, modem handshaking is used in some polled configurations, but in many cases it is not. In this case, when the channel is operating properly, all of the modem handshaking leads are at a steady-state logic level; thus, any change in the status of a lead provides information as to channel problem causes. A fault-isolation decision tree would be similar to that of Figure 3-1. The isolation of causes of parity errors in the computer-to-terminal protocol would also be similar to that of Figure 3-2 except for the use of information in the time domain (the same is true for isolation of high BER's in the message traffic).

At steps, in the fault-isolation process in Figures 3-1 and 3-2, in which transmitted and received pulse distortion was measured in the asynchronous network, timing information is observed in the synchronous network. Pulse jitter is observed on the send/receive data leads, timing jitter is observed on the send/receive clock leads (the clock frequency can also be measured), timing skew can be observed by comparing the data lead versus clock lead pulse transitions, and the synchronization status of the modem receiver can be obtained on the data quality lead (not shown on Figure 2-1, but part of RS-232C).

3.3 The Encrypted Mil Std 188-100 Synchronous Channel.

As shown in Figure 2-2, this interface does not permit as straight forward fault-isolation procedures due to the insertion of the crypto devices between the terminal/processor and associated modem, and the very few hand-shaking leads available for observation. Like the RS-232C synchronous channel, all control leads are at a steady-state logic level and any change indicates a problem. The following paragraphs are keyed to Figure 3-3, and start with a report from the computer operator that the terminal is down due to communications.

(a) First, observe the loss-of-carrier lead at the CAU/modem interface (at the processor end); is its status normal?

(b) If the status is not normal (carrier loss), observe the carrier signal level at the send line; if it is not present or at the proper level, the problem is in the send portion of the processor-end modem.

(c) If the send carrier is at the proper level, observe the received carrier level at the terminal end of the path. If it is not at the proper level, the problem is in the transmission path.

(d) If the receive carrier is at the proper level, observe the loss of carrier lead at the terminal end modem; if it indicates loss of carrier the problem is in the modem receiver.

(e) If the loss of carrier lead indicates the carrier is present (at the terminal end), we are at the same decision point as we were at step (b) at the processor end. For both cases, observe the data inhibit lead at the receiving end of the path. If it is normal (data not inhibited) the crypto is in sync and we must look elsewhere for the problem.

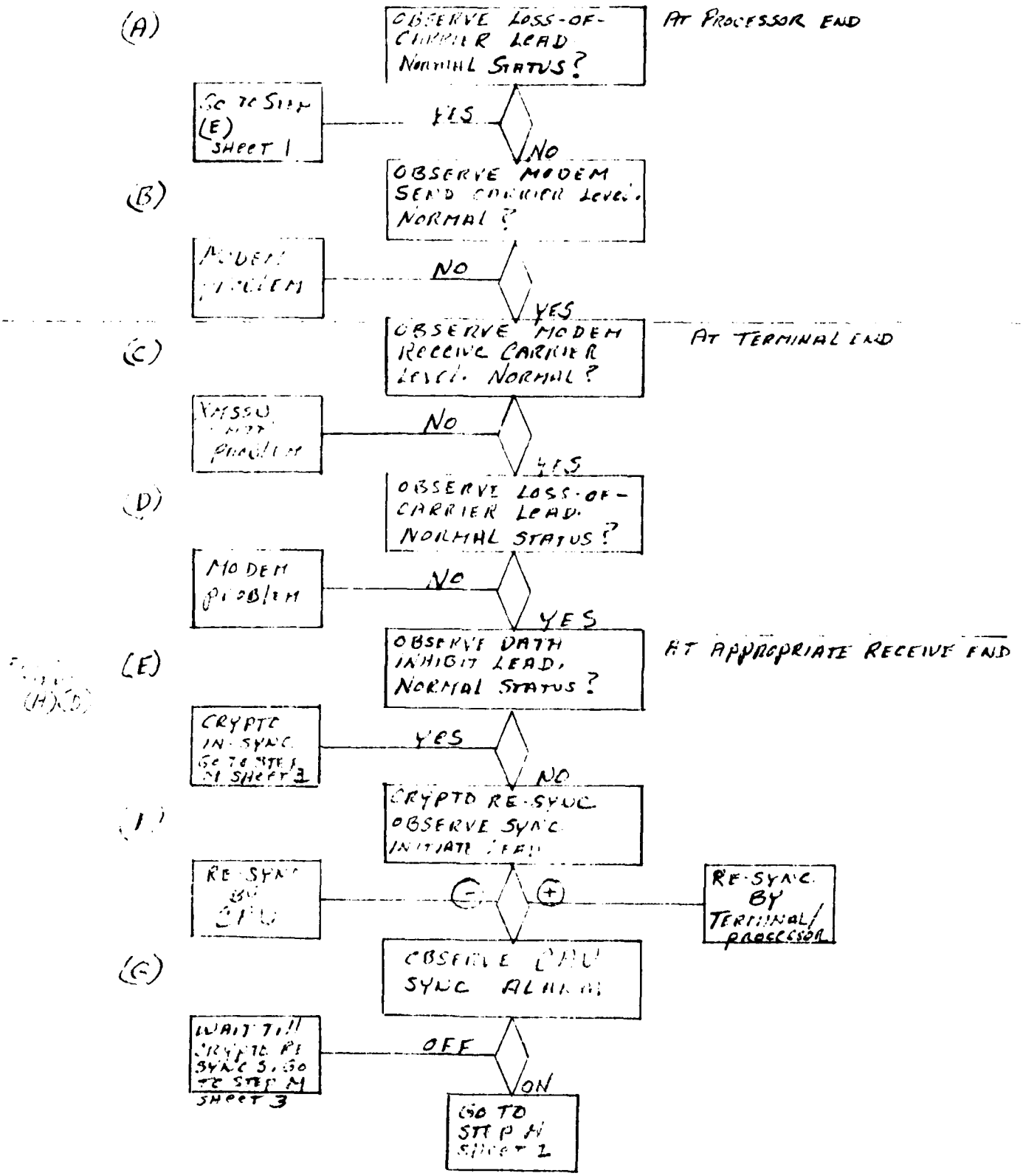


FIGURE 3-3 MILSTD-188-100 SECURE SYNC NETWORK (SHEET 1 OF 4)

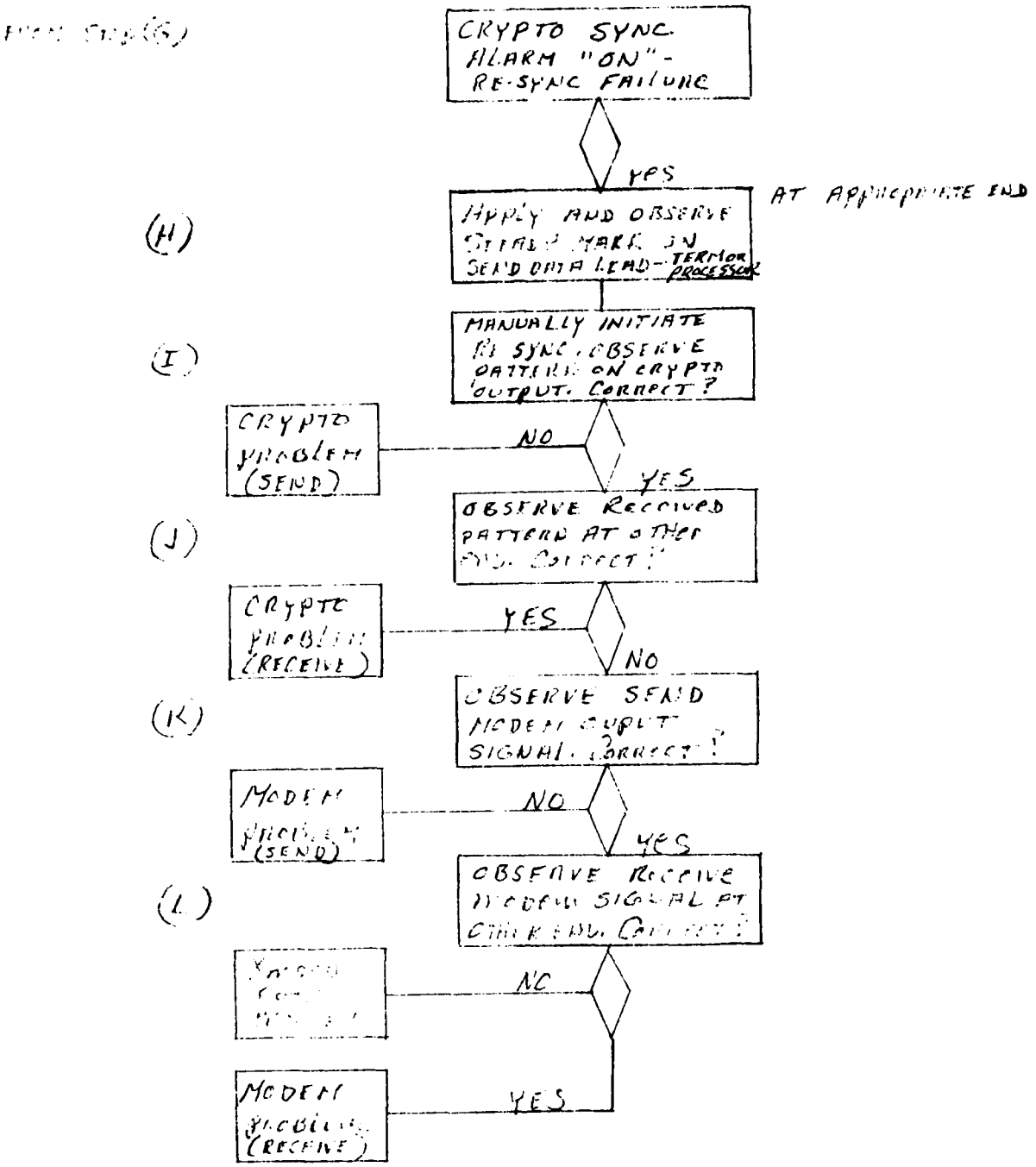


FIGURE 3-3 (SHEET 2 OF 4)

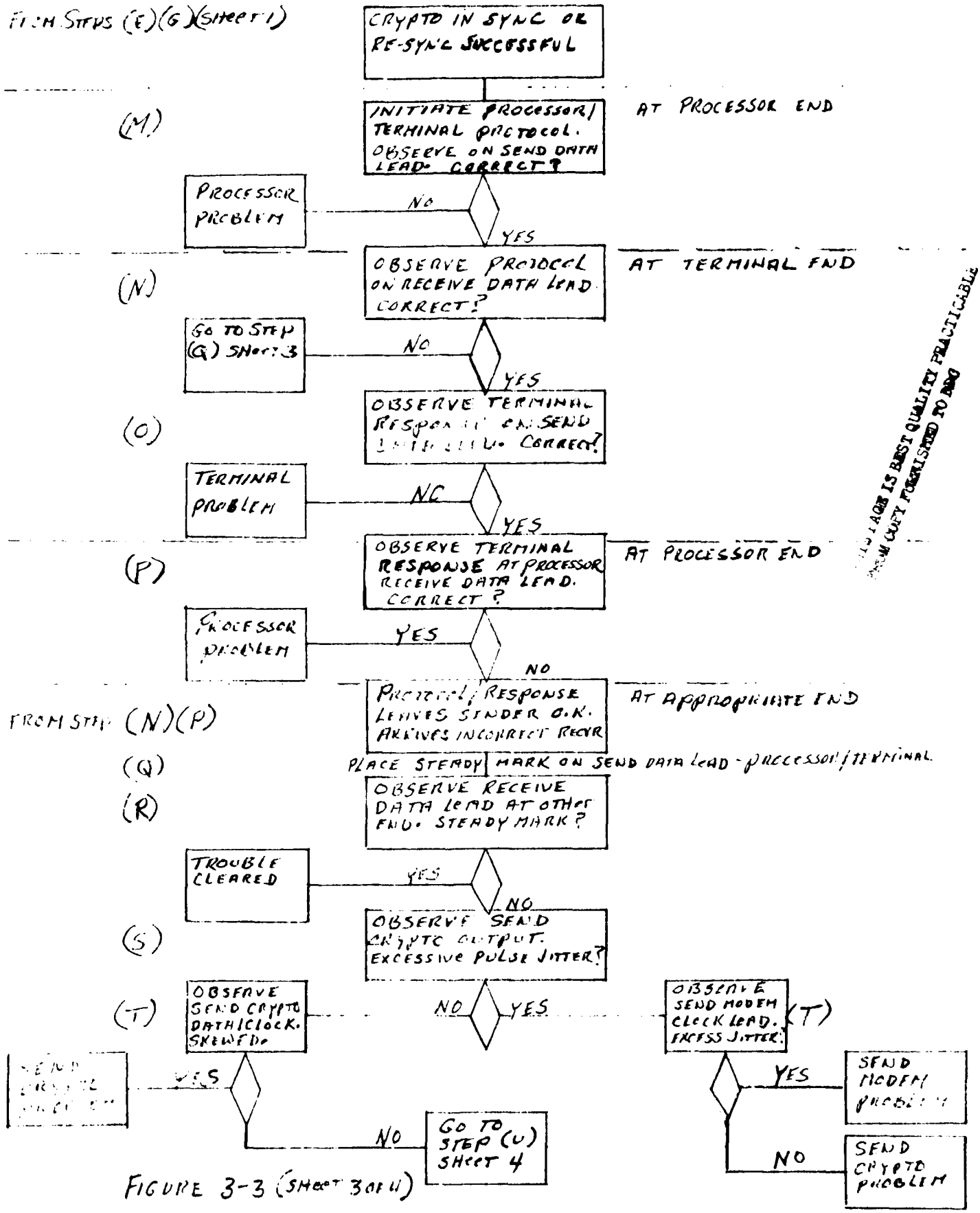


FIGURE 3-3 (SHEET 3 OF 4)

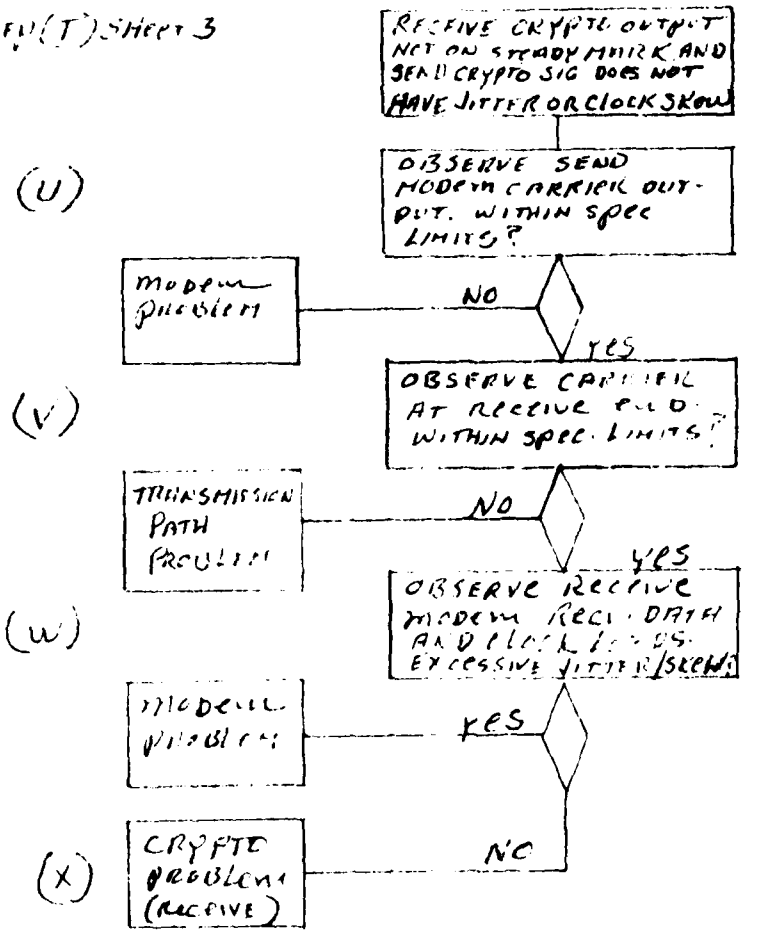


FIGURE 3-3 (SHEET 4 OF 4)

(f) If the data inhibit lead is "on" (data inhibited) the crypto is in its sync cycle; observe the sync initiate lead. If it is "on" re-sync was initiated by the processor/terminal; if it is "off", re-sync was initiated by the CAU.

(g) Observe the CAU sync alarm; if it is off and stays off, crypto has successfully gone through the sync cycle and data inhibit lead should go "off", in which case we are at the same point as step (e) with the data inhibit lead normal. If the CAU sync alarm is "on", the crypto sync was not successful.

(h) Apply (and observe) a steady mark on the send data lead (at processor or terminal to CAU interface).

(i) Initiate the crypto sync cycle and observe sync pattern on the CAU/modem send data lead. If the pattern is not correct, the problem is in the send crypto.

(j) If the send pattern is correct, observe the sync pattern at the modem receive data lead at the opposite end of the path. If the sync pattern is proper here, the problem is in the receive crypto.

(k) If the pattern is mutilated, observe the transmitted modem signal; if it is not within tolerance, the problem is in the transmitting modem.

(l) If the transmitted signal is proper, observe the signal at the receive modem input line; if it is not within tolerance, the problem is in the transmission path. If it is within tolerance, the problem is in the modem receiver.

(m) At steps (e) and (g) we had the situation where the crypto was not out of sync or it had re-acquired sync successfully (and the computer operator still could not communicate with the terminal). Initiate the processor-to-terminal protocol and observe the format/content on the processor send data lead. If it is not correct, the problem is in the processor.

(n) If the transmitted protocol is correct, observe it at the terminal receive data lead. If it is not correct, skip to step (q).

(o) If the received protocol is correct, observe the terminal's response on its send data lead. If it is not correct, the problem is in the terminal.

(p) If the terminal response is correct, observe this response at the processor receive data lead. If it is correct, the problem is in the processor.

(q) At steps (n) and (q) we had a correctly transmitted protocol which was received with errors. Apply (and observe) a steady mark to the appropriate send data lead processor or terminal).

(r) Observe the receive data lead at the opposite end of the path (processor or terminal). If this lead is at a steady mark, we have an intermittent problem that has cleared, or a marginal circuit.

(s) If the receive data lead is not at steady mark, observe the CRYPTO output send data lead (at transmitting end of path) for excessive pulse jitter (KG-series devices transmit a digital stream even though the input lead is at a steady-state level).

(t) If the jitter is excessive, observe the modem send clock lead for excessive jitter; if this jitter is excessive, the problem is in the modem transmitter. If the send clock lead does not contain excessive jitter, the problem is in the crypto. In step (s), if the CRYPTO send data lead jitter is not excessive, observe the CRYPTO send data lead versus the modem send clock lead for skew. If skew is present, the problem is in the crypto transmitter.

(u) In step (s), if the modem send clock does not contain excessive jitter and in step (t) if there is no skew in the crypto send data and the modem send clock, observe the transmitted modem signal on the line. If it is not within tolerance, the problem is in the modem transmitter.

(v) If it is within tolerance, observe the signal at the distant modem receive input. If it is not within tolerance, the problem is in the transmission path.

(w) If the received signal is within tolerance, observe the receive modem receive data and clock leads for excessive jitter and/or skew. If either is present, the problem is in the modem receiver.

(x) If neither excessive jitter or skew is present the problem is in the crypto receiver.

3.4 Summary/Conclusions.

a. There will be some "old" tech controllers among the readers of this who can visualize types of problems which would not yield solutions as readily as portrayed in the foregoing discussions. These kinds of problems are the network "gremlins" which are either intermittent in nature (everything checks out good while you are looking), or are a result of multiple problems of a marginal nature; i.e. two or more devices/paths are just within operating tolerances but together do not perform properly. However, the simplistic step-by-step type of approach discussed will isolate the majority of faults, and equipment substitution (as discussed in Section 4.0) can be used to isolate all but the most stubborn of "gremlins".

b. Based on the foregoing fault-isolation processes, it is apparent that all of the information (inherently available) is required to isolate network faults to the "which vendor" level. Some of the information is difficult to observe/measure and would require complex instrumentation operated by highly skilled technicians to do do. This, of course, is not in consonance with our objective of providing a capability for the computer operator to isolate problems. Some of the information is available at the remote terminal, and measurement/observation depending on actions by the terminal operator is also not in consonance with our objectives.

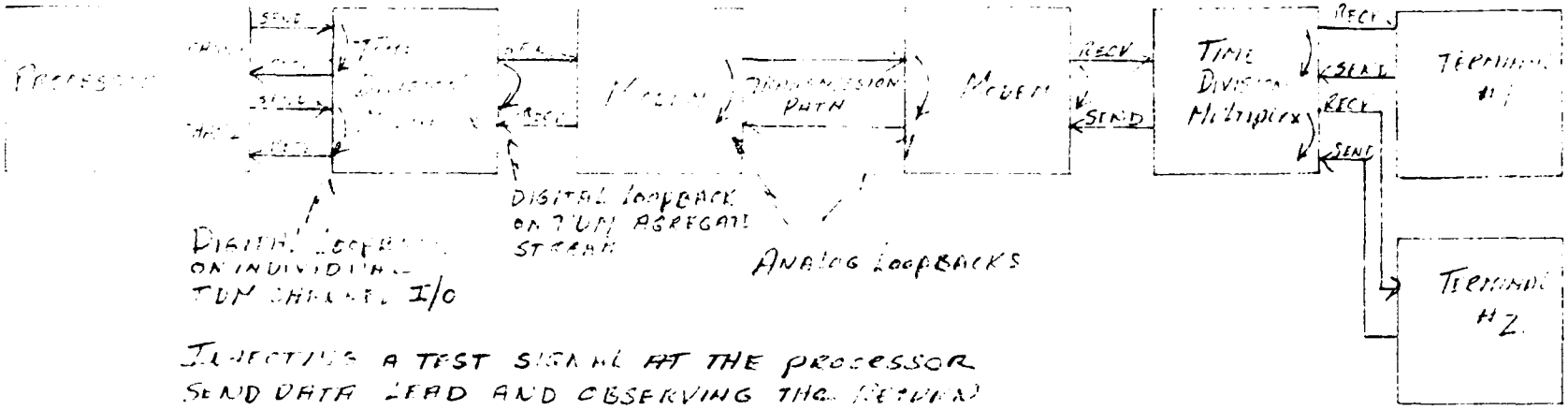
c. The following section (4.0) will discuss methods of extracting the required information while meeting the objectives of a single-ended fault-isolation capability which invites successful diagnosis by the computer operator. In some cases we will use negative logic; i.e. measure everything else and deduce that if everything else in the network is proper, the problems must be in the device whose parameters we could not measure. In other cases we will use device substitution and deduce that if the substitute device works and the primary device does not, the problem must be in the primary device. In still other cases we will emulate a device (especially processor protocol) or inject test signals with known characteristics which are easily observed for deviations.

4.0 EXTRACTION OF REQUIRED INFORMATION.

4.1 Loop-backs. One of our primary objectives is to provide a single-ended fault-isolation capability; i.e. one in which there is no requirement for actions at remote terminal or intermediate locations (e.g. crypto vault, multiplex node). Although it results in some ambiguities in the fault-isolation process, the most economical and practical method of meeting this objective is through the use of signal "loopbacks". With this technique a known test signal is injected on the processor send data lead, on a crypto send data lead, or on the modem send line (carrier output) and it is looped back at each interface point in the channel under test. The results are then observed on the appropriate receive lead at the processor end.

a. Figure 4-1 is an example of a channel with complete loopback capability. Injecting a test signal with known characteristics on the processor send data lead and observing the returned signal on the processor receive data lead as it is looped back at each successive interface can isolate many problems. In Figure 4-1, if a message with a specific bit content is applied to the send data lead and the returned signal on the receive data lead is observed for bit errors, we have a powerful fault-isolation tool. With a loopback at the TDM aggregate signal I/O, excessive errors on the receive channel lead would indicate a mux/demux problem. The ambiguity here is that we do not know whether the problem is in the multiplexing or demultiplexing function; but even with this ambiguity, we have determined "which vendor has the problem." If the TDM loopback returns a good signal, move the loopback to the modem analog lines. Excessive errors here indicate a near-end modem problem. If the returned signal does not contain excessive errors, move the loopback to the distant-end modem analog signal lines. Excessive errors here would seem to indicate that the problem is in the transmission path, but unless we have prior error-test data via this loop-back, this may not be so. The transmitted modem analog signal is traversing the transmission path twice (once in each direction); and even if the signal power losses are normalized with a loopback amplifier (at the distant end) the noise at the modem at the processor end of the path is the total of the noise in both directions of the path. This noise level is greater than that normally present at the modem analog receive line in a single direction path and will, of course, cause more bit errors to be produced by the modem receiver. However, if we have prior error rate data for the looped back transmission path when it is operating properly, a comparison can be made between new test results and the normal test data. This can then be used to determine if the transmission path is the problem. With good path results, the loopback is moved to the terminal end modem send/receive data leads. Excessive errors with this loopback indicate a distant end modem problem. If the channel is asynchronous, previous bit error test data taken when the channel is operating properly is required for comparison with the new test data. This is so because the pulse-time distortion in the processor-to-terminal direction of transmission is not corrected by the asynchronous modem receiver and is thus returned with the looped back signal where it is added to the distortion caused by the return path. With a synchronous channel this problem is not present since the modem receiver regenerates the digital signal. If the error rate is acceptable here, the loopback is moved to the final interface between the TDM channel I/O and the terminal. Excessive error rate here indicates a TDM problem; an acceptable error rate would indicate a terminal problem (assuming the original problem was not being able to raise the terminal or incorrect responses from the terminal).

b. In the above discussion we continued to "move" the loopback from interface to interface point. We certainly do not want to require our computer operator to physically move along the channel, nor do we want to depend on others to do so. These objectives cause us to reject two methods of providing loopbacks and selection of a third method. The rejected methods are manually activated and would require physical action at each interface point; i.e. loopback via patch panel or external switch circuitry at each



INJECTING A TEST SIGNAL AT THE PROCESSOR SEND DATA LEAD AND OBSERVING THE RETURNED SIGNAL ON THE RECEIVE DATA LEAD AS IT IS LOOPED BACK AT EACH SUCCESSIVE INTERFACE CAN ISOLATE MANY PROBLEMS.

FIGURE 4-1 LOOPBACKS IN THE PROCESSOR-TO-TERMINAL CHANNEL

interface or via built-in loopback circuitry within each device which is activated by manual switches. The selected method is via built-in loopback circuitry in each device which can be remotely activated from the processor end. Many modem and multiplex vendors offer devices with these features. The activation method can be that of manual switches on the processor-end devices which provide for activation of loopbacks at the processor, any intermediate node, and the distant terminal end of the channel. Some vendors also provide for remoting of all of the loopback controls to a common control panel. Built-in loopback circuitry can also have other advantages. One is normalization of the analog signal levels with a distant end analog loopback; i.e. the signal arrives at the distant end about 20 Db lower than the required transmit level. If the built-in loopback circuitry contains an amplifier with 20 Db gain, the returned signal leaves the distant end at the proper level. Another advantage for synchronous channels is that of buffering between the modem send/receive data and send/receive clock leads. The digital signal arriving on the distant-end modem receive data lead is clocked out by the receive data clock. This clock is derived from the average bit period of the incoming data stream and would not be expected to be in phase with the internal modem transmit clock which times the send data lead. A direct digital loopback at the distant-end modem send/receive data leads would result in an attempt to time the data with two clocks which are out of phase. An internal loopback buffer, which writes the receive data in accordance with the receive clock and reads it out in accordance with the send clock, solves this problem.

c. Two-wire communications channels present other loopback problems. A 2-wire half-duplex channel (transmission in both directions, but not simultaneously) does not permit use of loopbacks. This problem can be eliminated by using full-duplex modems over 4-wire circuits even though the terminal can only operate in a half-duplex mode. The standard RS-232C interface provides for this mode of operation. Low speed channel (up to 1200 b/s) full-duplex modems can be operated over 2-wire circuits, but this also presents problems (see below). Higher speed modems require use of a 4-wire circuit for full-duplex operation.

d. A two-wire full-duplex channel operates by using a different carrier frequency for each direction of transmission. Thus one modem transmits on frequency F1, and receives on F2 while the opposite end modem transmits F2 and receives F1. An analog loopback at the distant modem would thus return the wrong frequency carrier; i.e. return an F1 to a F2 receiver or vice versa. The cost of a second base wire-pair to convert to 4-wire operation seems a small price to pay for the fault-isolation capability gained. Even on long-haul leased common-carrier or DCS voice channels, a 4-wire channel costs only about 10% more than a 2-wire channel (since the trunks are already 4-wire and only the wire pairs at the tail ends are increased from 2-to 4-wire). In fact, elimination of the 2-to-4-wire hybrid improves circuit operation considerably.

e. A channel which contains crypto devices also presents loopback problems. If the TDM's in Figure 4-1 were replaced with cryptographic devices we would find that injecting a test signal on the processor send data lead and looping it back at the crypto/modem, modem/transmission path, distant transmission path/modem or modem/crypto interfaces would not produce a useable signal at the processor receive data lead. This is so, because the processor end crypto transmitter and receiver are not in bit or crypto sync with each other. Although some cryptographic devices will permit this to be accomplished, action by crypto maintenance personnel would be required; this would violate our single-ended computer center concept. A loop-back could be accomplished at the distant end crypto/terminal interface if it contained the send/receive data/clock compensation circuitry (buffer); however, the current inventory of crypto devices (including CAU's) does not provide this capability.

If a test signal is injected at the modem send data lead and observed on the modem receive data lead (with loopbacks at the modem/line, line/modem and modem/crypto interfaces), problems could be isolated to the modems and transmission path, or these could be eliminated as the source of the problem. Other techniques would be required to further isolate the problem to the cryptos or the processor/terminal (these will be discussed later).

f. In summary, we require loopbacks to meet our objectives. These loopbacks should be built-in each device and be capable of remote activation. All channels must use 4-wire circuits in order to accomodate loopback testing.

4.2 Patch Panel and Switch Matrix. All through Section 3.0 and in the above discussion on loopbacks, test signals were injected into the send side of a channel and observed on the receive side. These activities obviously require some means of access to the various interface circuitry. The observation of live traffic (versus test signals) requires that access to be on a non-interfering basis (i.e. by a high-impedance bridged circuit). Based on the use of loopback circuitry, access to the various signal circuits is only required at each interface at the processor end of each channel; each access must provide the capability to monitor (in service/non-interfering) and to seize (out-of-service) each interface for testing purposes.

a. These capabilities can be provided by patch panels or switching matrices. Switching has the advantage of being easier to use and less prone to operator error than patching. If a remotely addressable switching matrix is used, scanning techniques can be used in which each circuit is sequentially selected, the signals present are measured, and the values then compared against stored threshold values. This technique can provide trending analysis which can detect gradual degradation and thus do some "predicting" of problems. Patch panels have the advantage of being less costly than switching. The average EIA RS-232C interface requires access to 12 of the possible 25 leads; and the transmission path interface is 4-wire, thus requiring 16 access points per channel. Patching for 12 channels can be purchased for about $1500. Switching (manual activation) for 12 channels for the 16 access points to a single test trunk) costs about $6000. Remotely addressable switching would cost somewhat more for the decoder plus the cost of the scanning hardware/software to drive it. The patch panel also permits cross-patching (alt. routing) and equipment substitution to be accomplished at the same cost estimate, whereas including these capabilities in a 12-channel switching matrix would increase the cost about 10 times.

b. In a secure (encrypted) network, two independent patching or switching facilities are required (one on the unencrypted side and one on the encrypted side of the crypto devices), and both must meet Tempest criteria. The total cost increases to about 4 times that for non-secure systems; 2 times since two patch/switch facilities are required and 2 times to meet Tempest.

c. In networks which include TDM's (as shown in Figure 4-1), the patching/switching capability must be larger than the number of terminal channels in order to provide access to the aggregate bit stream (multiplexed side) of each TDM; e.g. if each TDM could handle 6 channels, two TDM's are required for 12 terminals and the number of patch/switch channels required is 14 (12 channels plus 2 TDM streams).

d. In summary, access for signal monitoring on a non-interfering basis, and access for seizing a channel for out-of-service testing is required;

(1) For a non-secure, non-multiplexed network, one digital and one analog patch/switch is required for each channel.

(2) For a secure, non-multiplexed network, two digital and one analog patch/switch is required for each channel.

(3) For a non-secure, multiplexed network, one digital patch/switch is required for each channel, and one digital and one analog patch/switch is required for each TDM aggregate bit stream.

(4) For a secure network with multiplexing (not discussed above) the patch/switch requirements depend on the crypto/TDM configuration used; i.e. are the individual channels individually encrypted and the encrypted streams then multiplexed, or are the individual channels multiplexed first and the aggregate bit stream encrypted?

4.3 Modem Handshaking. In Section 3.0 during the modem handshaking fault isolation discussion (Figure 3-1), the computer operator was required to initiate the processor routine (in fact to accomplish the various steps in Figure 3-1, the handshaking routine would have had to be exercised several times). In most networks this would interrupt other processing tasks and is thus an unsatisfactory approach. The handshaking routine need only be accomplished once by the processor itself in order to determine that the processor hardware/software is operating properly. Once this determination is made, repetition of the routine can be accomplished by a device which emulates the processor.

a. There are commercially available devices which permit an operator to place logic voltage on outgoing leads of the RS-232C interface and to detect logic voltage on incoming leads. The logic voltage is placed on outgoing leads by means of manually operated switches on straps; incoming logic voltage if detected and displayed via LED circuitry usually biased to operate when the logic voltage exceeds the RS-232C ± 3 volt non-operating limits. While this method of exercising the control leads would be adequate in synchronous configurations (in which all leads remain at steady-state values), it would not be adequate for configurations which go through a timed-sequence routine.

b. To emulate a timed-sequence routine, the emulation device must place logic voltages on outgoing leads in the proper timed-sequence, monitor this sequence to determine that it is, in fact, correct, and then monitor the logic voltages on incoming leads for correct timing and sequence. The entire handshaking routine is usually accomplished in a matter of a few hundred milliseconds; thus, the emulator must store the results and display them after the routine has been completed. This storage could be in a microprocessor memory for one-time observation or it could be on floppy-disk or magnetic tape cassette so that a repetitive series of handshaking attempts could be analyzed. This latter capability is especially useful in isolating intermittant problems and for recording any changes in the lead status during actual or test traffic flow.

c. In summary, a device is required which can monitor the handshaking routine as it is accomplished by the processor and terminal, and which can emulate either the processor or the terminal in the handshaking routine. The results on each monitored and emulated routine attempt must be compared against the correct time-sequence and then displayed for operator analysis. It is also desirable that the device provide the capability to store the results of several routine attempts for subsequent comparison and analysis, and to store the status of each lead (and changes thereto) during traffic flow (actual or test). To accommodate different routines, the device should be programmable.

4.4 Processor-to-Terminal Protocol. In Section 3.0 (Figure 3-2), during the protocol fault-isolation discussion, the computer operator was required to initiate the processor-to-terminal protocol many times. This is considered to be unacceptable since it interrupts

the computer operations. For the purposes of fault-isolation, one attempt by the processor is sufficient to determine if the processor is exercising the protocol correctly. What is required is a device which can monitor the protocol (in both directions) when it is being exercised by the processor, and that can emulate the protocol in either direction (i.e. act like the processor and attempt to raise the terminal; or act like the terminal and respond to the processor). There are commercially available devices which provide for setting up of several character long sequences (by setting of individual switches for each bit) and releasing of the sequence by operation of a transmit key. Monitoring of received character sequences is also on a bit-by-bit basis (via illumination of a lamp or LED for each bit). These devices fall short in several ways. Since there are many possible protocols (and even many possible options within a single protocol method), a programmable device is needed so that the desired protocol can be selected by simple command. The monitor function must evaluate the timing of the sequences as well as the content and convert those normally non-printable characters (control symbols) to some form of readily identifiable symbology for display purposes. The display should present both directions of transmission simultaneously and also monitor and display the status of the handshaking leads during the protocol exchange. A method of storage for the results of several attempts to permit subsequent analysis is also desirable.

4.5 Traffic Flow Errors.

In Section 2.0 we discussed the value of the information available in the normal traffic flow. In each network the message formats are fixed and errors in format can be observed for patterns of errors which when consistant usually indicate problems in the source device. It was also discussed that observation of parity error frequency can provide a pseudo-error rate figure; the frequency of ARQ's is also indicative of the error rate. The same device used to monitor the processor/terminal protocol could be used to monitor traffic in both directions; the display should be large enough (number of characters/lines) to accommodate the message formats used. It should provide a method of indicating characters with parity errors, and to accumulate the number of parity errors in a message. It should display symbols to indicate ARQ's and accumulate their number. It is also desireable to be able to record traffic for subsequent error pattern analysis.

Sometimes it is helpful in fault-isolation to be able to exercise a distant terminal (especially when loopback tests indicate the received signal at the terminal is correct); a simple method of doing this is to be able to send a test message to the terminal which forces it to perform all of its functions. Thus, it is desireable that the traffic monitoring device have the capability to transmit pre-formatted test messages.

Another related capability which is required to isolate modem/transmission path problems, is that of a bit-error-rate test (BERT). Whereas observation of parity errors and ARQ's provides a pseudo-bit error rate measurement, BERT provides a precise error rate measurement over the transmission path. A pseudo-random bit pattern is transmitted and compared at the receiver (which has apriori knowledge of the transmitted pattern); the bit errors in the received signal are counted and displayed as the ratio of bits in error to the number transmitted. This precise measurement is especially useful on a marginal or intermittant circuit since the identical test can be repeated.

During monitoring of live traffic, transmission of test messages, and BERT, the handshaking lead status should be monitored for changes.

4.6 Quasi-Analog Signals.

Several steps in Figures 3-1, 3-2 and 3-3 required measurement of the level of the analog signal at the modem transmitter and receiver. Several other steps required measurement of the quality of the transmitted and received modem analog signal.

a. By means of distant-end loopbacks we can easily determine if the levels of the signals are correct, and even determine if incorrect levels are caused by the modems or the transmission path. In Figure 4-1, if we cause the processor-end modem to turn on its carrier, its level can be measured with a common DBM meter. If the distant-end modem has a built-in analog loopback circuit containing a fixed gain loopback amplifier, measurement of the signal level at the processor-end receive signal line will indicate the total loss (both directions) over the transmission path. If the transmission path loss is normal, a loopback at the digital side of the distant end modem, and measurement of the carrier level at the processor-end signal line will indicate the distant end modem transmit carrier level.

b. The more difficult problem is measurement of the quality of the modem analog signals. There are several parameters which require measurement (power spectrum, S/N ratio, intersymbol interference), and each requires rather complex test instrumentation, the operation of which, does not meet our objective to permit the computer operator to isolate faults. We can, of course, substitute another modem (via patching) at the processor-end, but this would not permit isolation of faults between the distant modem and the transmission path. Another method would be to measure the quality of the transmission path in conjunction with near-end modem substitution, but these measurements (frequency response, delay characteristics, noise, etc) also require complex instrumentation.

Fortunately, Bell Labs developed a measurement technique, called PAR (peak-to-average-ratio), which permits a relative figure of merit to be measured over a transmission path. (3) Devices to make this measurement are available commercially and usually include signal and noise level measurements in addition to the PAR meter function. The PAR transmitter transmits an analog signal of precise level and frequency content on a precise pulsed basis. This signal has a specific ratio between its peak power and its average power. This signal is looped back at the distant-end modem analog signal lines and received by the PAR receiver at the processor end. All of the anomalies in the transmission path lower the peak-to-average ratio, and while it does not indicate why, it does provide the means to isolate the fault to the transmission path. Combining the PAR test with substitution of the near-end modem can then isolate problems to either modem and the transmission path. The PAR meter is simple to operate and the results require no interpretation other than comparison of the current meter reading (0 to 100) with previous PAR meter readings taken when the channel was operating properly.

c. In summary, a PAR meter in conjunction with the capability to patch/switch-in a near end substitute modem is required to isolate faults in the analog subsystem.

4.7 Digital Signals.

Several steps in Figures 3-1, 3-2 and 3-3 required measurement of the quality of the digital signals on send and receive data leads, measurement of the pulse jitter on data and clock leads, and a comparison of data lead/clock lead transition periods.

a. On asynchronous channels the receive signal is demodulated to a digital signal without regeneration (re-timing); i.e. all of the transmission path characteristics which cause the analog signal to be degraded are directly reflected in the demodulated digital signal in the form of pulse-time distortion. Each pulse is lengthened or shortened in relation to its proper length. This pulse distortion can take many forms depending on the underlying causes; i.e. individual pulses can be distorted in a random sort of manner, strings of pulses can be distorted in a similar manner, pulse distortion can occur at leading edges, trailing edges, or both, mark pulses (logic ones) can be distorted in one manner and space pulses in another, etc. However, for our fault isolation objective, we need only know whether or not the digital pulses are distorted, and if the distortion exceeds that which is normal for the circuit under test. Most commercially available digital distortion

analyzers generate a known signal and compare the length, leading and lagging edge transition periods of the received signal against this reference signal. The operator can select the type of distortion to be measured (bias, end-distortion, switching, average and peak), and the result is displayed in terms of a percentage; the amount of time pulses are lengthened or shortened versus a theoretically perfect pulse. With the switch set for "average", the display reflects the average amount of time the pulses in the digital signal are distorted. Although this can be a very useful measurement, intermittent bursts of high value pulse distortion are averaged in with the long term average distortion and are not readily apparent to the operator; and this type of anomaly is very often present on faulty transmission paths. With the analyzer switch set for "peak", the read-out represents the highest value of pulse distortion measured over the test period. Most analyzers also provide outputs to drive a dual-channel strip chart recorder to record the "average" and "peak" distortion along a common time-of-occurrence base.

b. For our purposes, a capability to measure "average" and "peak" pulse distortion, in conjunction with loopbacks and PAR/meter tests, can be used to isolate pulse distortion problems on asychronous channels to the modem at either end, or the transmission path.

c. On synchronous circuits, the modem receiver regenerates the digital signal by recovering the data clock period from the average transition period in the data stream; each data pulse is then clocked out to the sink in accordance with this receive data clock. Thus each digital pulse is made to be the same length as every other pulse and very near to the length of a perfect pulse. The digital distortion analyzer would indicate little or no "average" distortion. However, it will indicate changing values of "peak" distortion on both the data and clock leads. What is actually being measured is clock and data pulse jitter which alternatively changes the position of the pulse edge around its proper position. This jitter is a function of the timing recovery process and is normally at a very low value (percentage of total pulse length in time), but under severe transmission path conditions or modem malfunction, the value, as indicated by a "peak" digital distortion meter, will rise considerably.

d. Another required measurement on synchronous circuits is that of comparing the clock lead pulse transition relationship to that on the corresponding data lead; i.e. the negative going transition on the clock stream should occur at center pulse on the data lead. The normal method of making this comparison is by observing both signals simultaneously on a highly accurate dual-trace oscilliscope. This method does not meet the objective for use by the computer operator. However, there are BERT sets which include an adjustable "sampling window" which, although not as accurate as the oscilliscope method, do provide an excellent method of determining if the data/clock relationship is within prescribed limits.

e. In summary, for digital measurements, the methods available and required are a digital distortion measurement which indicates, at least, "peak" distortion, and preferrably "average" and "peak" distortion. Also required is a BERT measurement which includes an adjustable "sampling window". Loopbacks are used to isolate the source of the digital signal problem in conjunction with the analog signal measurements.

4.8 Information Required Versus Methods of Extraction.

Thus far the following methods of extracting network information have been determined to be required to meet the objectives of a single-ended, computer operator capability to isolate problems to the responsible vendor as represented by a "block" in a system block diagram (a device or link);

a. Built-in remote controlled analog and digital loopbacks in modems and multiplexers.

b. All transmission circuits operated on a 4-wire full-duplex basis even though the terminal operates in a half-duplex mode.

c. Patching/switching at each digital and analog interface at the processor end of the channel, including the capability to swap modems at the processor end. The patch/switch matrix must permit monitoring of all leads on a bridging basis and permit breaking of all leads and seizing them for testing in both directions of transmission.

d. A device which can monitor, analyze and store the results of modem handshaking routines as they are accomplished by the processor and associated channel modem. The device must also be capable of emulating the routines and to analyze and store the results of such emulated handshaking exercises.

e. A device which can monitor, analyze and store the results of processor-to-terminal protocol (in both directions). The device must also be capable of emulating this protocol (as processor and terminal) and analyze and store the results of such emulated protocol exercises.

f. A device which displays live traffic with a sufficiently large display to permit observation of either a total message or of a total message page in order that error patterns can be observed.

g. A device with the capability to count and store the occurrence of parity errors and ARQ's.

h. A device with the capability to transmit preformatted test messages.

i. A Bit Error Rate Tester (BERT) with the capability to adjust the center-pulse sampling window.

j. A device which can measure analog signal levels and accomplish the peak-to-average ratio test (PAR).

k. A digital distortion measuring set with the capability to measure "peak" pulse distortion (the capability to measure "average" distortion is not required, but is desirable). It should be arranged to measure data and clock signals.

4.9 Review of Fault-Isolation Procedures. Now let us review the fault-isolation procedures in Figures 3-1, 3-2, and 3-3 and use the methods/device capabilities discussed above and determine if any additional capabilities/methods are required.

4.9.1 Asynchronous Network Modem Handshaking (Figure 3-1).

a. Steps (1), (2), (3), and (4) consist of observing the status of certain modem handshaking leads at the processor end. This can be accomplished via the patching/switching capability and the modem handshaking monitor/emulator.

b. Step (5) requires measurement of the processor end modem send carrier level. This can be accomplished via the patching/switching capability and the PAR test set.

c. Steps (6) and (7) require measurement of the modem carrier level as received at the distant end. This can be accomplished at the processor end via the patching/switching capability, the PAR test set and the built-in remote loopback (with fixed gain amplifier) on the line side of the distant modem.

d. Steps (8), (9), (10), (11), (12), and (13) involve observation of the time lag between certain events in the modem handshaking routine at the processor end and measuring the levels of the send and receive carriers at the processor end. These can be accomplished via the patching/switching capability, the modem handshaking/emulator device and the PAR test set.

e. Step (14) requires measurement of the received carrier level at the distant end. This can be accomplished via the patching/switching capability, the remote modem line-side loopback and the PAR test set.

f. Steps (15), (16) and (17) require observation of the time lag between certain events in the modem handshaking routine at the distant end, in conjunction with steps (18) and (19), in order to isolate the fault (terminal does not respond to processor query) to either the terminal, distant end modem, or transmission path. Specifically the requirement is to determine if the remote modem turns its carrier detect lead on in the proper time frame, does the terminal have its data terminal ready lead on and does the remote modem turn its send carrier on in the proper time frame. This information is necessary to determine why the carrier received at the processor end modem is arriving within a time frame which exceeds that permitted by the processor time-out period. Steps (18) and (19) require observation of the carrier level as it is received at the processor end and observation of its time of arrival in relation to its time of transmission from the distant end. Direct observation of the handshaking lead status at the distant end is not possible unless we have a monitor at the distant end which detects the time/sequence of the change in status of the leads; and operation and observation of such a monitor by the remote operator violates our single-ended fault-isolation objective. The remote monitor could be configured to report the status to the central facility via a sub-carrier over the data transmission path. However, the cost of having such a monitor at every remote terminal would be large. There is a means to indirectly observe the status of the distant end handshaking leads, and although under some circumstances could result in ambiguous results, will provide the correct diagnosis most of the time. If the handshaking emulator is arranged to turn on the processor end request-to-send lead (via patching/switching capability) and calculate the time elapsed between this event and time at which the processor end carrier detect lead turns on, isolation of faults at the distant end can be accomplished as follows:

(1) Observe the elapsed time between the events with a remote loopback on the line side of the distant modem and compare the observed time with the normal time period (established by previous tests when the circuit was operating normally). If the observed time is excessive, the problem is in the transmission path (either or both directions). This situation occurs occasionally on leased long-haul circuits when the common carrier temporarily alt-routes the channel for maintenance or traffic load balancing purposes. For example, a Chicago, IL to St. Louis, Mo. link is alt-routed via Los Angeles, Ca. and the signal propagation time is lengthened by the increased path length, the change in path medium (LOS radio to coax), and the addition of 20 additional mux/demux nodes. Although the total round-trip addition to the propagation time may only be on the order of 10 - 15 milliseconds, this can be significant if the processor time-out period is set very near the normal turn-around time of 200 - 300 milliseconds.

(2) If the time period observed in the above step is normal, move the distant end loopback to the digital side of the distant modem and repeat the test. Excessive time in this step indicates a distant modem problem. Normal time indicates a terminal problem. This test does produce an ambiguity in that with the distant end modem digital side loopback, the status of the remote terminal leads (data terminal ready and request to send) are ignored by the modem. The status of these terminal leads could be proper and the problem could be in the modem logic circuitry which detects and acts on the status of these leads. This ambiguity seems a small price to pay when compared with the cost of having a remote handshaking monitor at each terminal.

g. Steps (20) and (21) require measurement of the total handshaking routine time-period and comparing it with the processor system specified time-out period and measuring the actual processor timeout period versus the specified period. Both of these tests can be accomplished at the processor end via the patching/switching capability and the handshaking emulator.

4.9.2 Asynchronous Network Processor to Terminal Protocol (Figure 3-2).

a. Steps (1) through (5) require exercising the protocol and observing it as sent by the processor for format, content and parity errors. The response from the terminal is then observed for format, content, parity errors and time of arrival (versus processor time-out period). All of this can be observed and measured at the processor end via the patching/switching capability and the protocol monitor/emulator device.

b. Steps (6) and (7) involve observing the processor protocol message as it is received at the distant terminal and observing the terminal response as it leaves the remote terminal. Since these observations cannot be accomplished directly without remote monitors at the terminal, indirect methods must be used.

(1) By observing the processor protocol as it is transmitted (via patch/switch and protocol monitor/emulator), looping it back at the line side of the distant modem, and observing it for errors as it is received back at the protocol monitor/emulator, we can partially isolate the problem. If it is returned with errors (during several attempts), the problem could be in the processor end modem or the transmission path. By substitution with another processor-end modem, the fault can be isolated to the modem or the transmission path.

(2) If, in the above test, the protocol message is returned error free, move the loopback to the digital side of the distant modem and repeat the test. If the looped back message contains errors, the fault is in the distant modem; if it is error free, the problem is in the distant terminal.

(3) In some cases it would not be necessary to accomplish the tests in (1) and (2) above; e.g. if in the observation of the terminal response in steps (1 through 5) the terminal response contained a format or content error which appeared in the same manner on every attempt, the problem is obviously in the terminal since the modem and transmission path error patterns tend to be random in nature.

c. In steps (6) and (7), above, the observed protocol messages either contained errors or were error free. In many cases, this decision is not so clear cut; i.e. sometimes there are errors and sometimes there are no errors and additional tests are required to isolate the fault. Steps (8) through (10) accomplish these tests and may be applied to either direction of transmission.

(1) In the processor to terminal direction, the digital distortion at the output of the processor is measured via the patch/switch capability and the distortion test set. If the distortion exceeds the specified limits, the problem is in the processor line driver. If it is within the limits, loop the signal back at the digital side of the distant modem and measure the distortion at the processor and receive data lead. If the distortion is within the pre-determined limits for the looped-back round trip, the problem is in the remote terminal. If it exceeds those limits, move the loopback to the line side of the distant modem and repeat the test. If the measured distortion is within the established limits, the problem is in the distant modem. If it is not within limits, swap the processor end modem and repeat the tests, which then isolates the problem to the processor end modem or the transmission path. An additional test with the PAR meter can be used to confirm transmission path problems, especially when the results of the previous tests are erratic (step 10A). The PAR signal is transmitted on the transmission path directly via the processor end analog patch/switch capability, looped back at the line side of the distant modem and measured at the processor end signal line. This test measures the quality of the transmission path directly (without modem or source/sink circuits, except for the loopback amplifier) and can isolate true transmission path problems versus apparent problems/caused by injection of noise or interfering signals by the normally connected devices. In addition, the common carriers understand PAR tests and are more willing to accept those results as being correct.

(2) In the terminal-to-processor direction, a more indirect approach is required. Step (8) requires measurement of the pulse distortion of the terminal response as it is transmitted from the terminal. Instead skip to step (9) and measure the pulse distortion of the terminal response as it is received at the processor. If it is within limits, the problem is in the processor receiver. If it exceeds limits, swap modems at the processor end. If the problem was not cleared with the substitute modem, test the transmission path with the PAR test set. If this does not indicate a transmission path problem, initiate a loopback at the distant modem digital side; distortion within limits indicates a terminal problem. If the distortion exceeds limits, loopback on the signal line side of the distant modem; distortion within limits indicates a distant modem problem. The PAR test was not absolutely required to isolate the problem if the distortion measured is relatively constant and clearly within or exceeding the established limits. PAR confirms and re-enforces the diagnosis when distortion values fluctuate widely or are intermittant in nature.

4.9.3 Secure Synchronous Network (Figure 3-3).

There are three major differences, in this network as compared to the asynchronous non-secure network. One, obviously, is the addition of the crypto/CAU devices to the equipment lineup and the associated problem of not being able to use loopbacks at the clear text side of the crypto device. Another difference is the synchronous mode of operation which requires additional measurements to be made concerning the timing/clock. The third difference is the lack of a modem handshaking routine and the wealth of information provided by that routine. There are three control/status leads which provide some network information. The latter two differences (timing and handshaking) could also apply to a non-secure synchronous network. These differences, especially the crypto/CAU, force us to use indirect approaches to fault-isolation procedures which meet the primary objectives of single-ended operation by a computer operator. In Figure 3-3, the reported problem is that a terminal will not respond to the processor.

a. Step (a) requires observation of the status of the modem loss of carrier lead at the prcoessor-end. This can be accomplished at the black patch/switch with the handshaking monitor.

b. Step (b) requires measurement of the processor end modem transmit carrier level. This is done via the audio patch/switch with the PAR test set.

c. Step (c) requires measurement of the carrier level as it is received at the terminal end. Here a loopback (with a fixed gain amplifier) at the line side of the distant modem is used, the level is measured at the processor end receive line, and compared with the normal looped back level.

d. Steps (d), (e), (f), (g), (h), (i), and (j) require observation of the crypto/CAU control/status and data leads at both the processor end and the terminal end. At the processor end, these leads could be observed via the handshaking and protocol monitors. Under our single ended fault-isolation objective, the status of these leads at the terminal end cannot be directly observed, but the terminal end CAU essentially does this for us and reports the net results to the processor-end CAU. (4) When the processor end CAU initiates re-sync and three such attempts fail, the remote CAU transmits a message to the local CAU which summarizes the status of the remote crypto. The local CAU will activate one of two alarms; "master alarm" which indicates that the problem is in the local crypto or the modem/transmission path; or "remote alarm" which indicates the problem is in the remote crypto or the modem/transmission path.

e. Steps (k) and (l) require observation of the modem lineside output/input signals at both ends of the circuit. The signal levels can be measured directly at the processor end and indirectly via loopback at the distant end. The quality of the signal (spectrum, etc) must be determined indirectly; i.e. the transmission path can be determined to be or eliminated as the source of the problem via the PAR test. The local modem can be determined to be or eliminated as the cause via modem swapping.

f. Steps (m), (n), (o), and (p) require exercise and observation of the processor to terminal protocol at both ends of the circuit. In the asynchronous non-secure network, observation of the protocol at the distant end was accomplished at the processor end via loopbacks on both sides of the distant modem. In a non-secure (no crypto) synchronous network this could be accomplished in a similar manner via the built-in loopback timing buffer in the modem. However, with the crypto in the circuit we cannot accomplish a loopback from processor-to-the line or digital side of the distant modem since this would result in a circuit with the crypto in the circuit at the processor end only. We also cannot use a loopback at the crypto to distant terminal interface unless we add such a capability to the crypto/CAU, including a send/receive clock/data buffer. Instead, an indirect approach is used; it has been previously determined that the crypto/CAU's at both ends are in sync and operating properly; it has also been determined (via PAR tests and modem swapping) that the transmission path and modems are operating properly (except for timing and bit error problems). The next step is to observe the protocol as it is transmitted and received by the processor via the protocol monitor to eliminate or determine that the processor is the problem. If it is not, we connect the protocol emulator/monitor via the Black Patch/Switch (eliminating the processor end crypto) and emulate the processor protocol. This protocol is looped back at the digital side of the terminal end modem (eliminating that crypto/CAU) and observed for content/errors. If it does not contain errors, the distant terminal is the problem.

g. If the above test shows errors in the looped-back protocol, steps (q), (r), (s), (t), (w), and (v) attempt to isolate the source of the errors by observing pulse jitter on the send/receive data leads (crypto/modem interface) and the clock pulse/data pulse alignment at both ends of the channel. Steps (u) and (v) assess the quality of the modem analog signal and are accomplished in the same manner as in steps (k) and (l). Pulse jitter can be observed directly at the processor end via the RED patch/switch and the peak pulse distortion measurement. Pulse jitter at the distant end can be observed indirectly via loopbacks on both sides of the distant modem. Timing skew at the local crypto/modem interface can be isolated via the red patch and the BERT device (with an adjustable

sampling window in its receiver). The BERT pattern is transmitted on the local modem send data lead and looped back at the digital side of the distant modem. The BERT sampling window is reduced in length until the receiver is making all error decisions. This window length is compared with that obtained when the circuit was operating normally. If the window length value is normal, the problem is in the local crypto. If it is not normal, move the loopback to the line side of the distant modem. If it is now normal, the problem is in the distant modem; if it is still not normal, swap modems at the processor end. If it is now normal, the problem was in the local modem; if not, the problem is in the transmission path.

b. It would appear that we have sometimes eliminated the modems and transmission path as problems (via PAR and signal level loopback tests and local modem swapping) and then later determined that either the modems or transmission path are the problem (via pulse jitter BERT sampling window, and modem swapping). This apparent conflict is due to the limitations of the PAR tests. While the PAR test does provide an overall measurement of the capability of the transmission path, it can give false indications with regard to certain problems and under certain conditions. The primary condition under which PAR is inaccurate is when measuirng a short tail circuit (such as from a base to an AUTODIN switch) which is heavily conditioned within the transmission path (e.g. AT&T 3002 voice channel with C-4 conditioning). The ripple content in the conditioned envelope delay curve has been found to produce serious errors in PAR readings. This problem should not have much impact on new processor networks since most of the new high-speed synchronous modems are microprocessor based and accomplish the required equalization automatically within the modem. Another parameter which can cause erronious PAR readings is the presence of phase-jitter which is accumulated along the transmission path. This phase jitter is reflected in the modem receiver and when added to the normal timing jitter produced by the modem timing recovery circuitry, can result in excessive pulse jitter in the received data stream. This combination of causes of the excessive pulse jitter would not be detected by the PAR test.

4.9.4 Some General Comments.

a. The methods discussed in this section leave us with one ambiguity in both of the networks considered; i.e. the status of the distant modem carrier detect lead. If tests using the loopback on the digital side of the distant modem were successful we assumed that the problem was at the distant terminal (or crypto). However, with this type of loopback the status of the carrier detect lead is ignored in most modems. Thus it is possible that although the carrier is present at the distant modem receiver, the carrier detect lead driver is defective. This would be interpreted by the terminal as no carrier present and it would not respond to anything on the receive data lead. The expense of providing a monitor with the capability to transmit the status of the carrier detect lead back to the processor end does not appear justified, in view of the fact that this particular malfunction does not occur often. Also, most modern modems include a front-panel indicator for this lead. On these rare occasions when the remote modem carrier detect function is suspect, the terminal operator could observe the status of the carrier detect indicator lamp (off/on). This, of course, technically violates the single-ended fault-isolation concept, but in this case what is being done by the terminal operator requires no technical capability and the alternative (automatic monitor) is not cost effective.

b. When multiplexers are inserted in the equipment lineup, the fault isolation procedures are changed from that discussed, but only to the extent that tests must be repeated at the interfaces on both sides of the multiplex equipment. At the processor end this can be accomplished via the patch/switch capability; at the distant end this can be accomplished via loopbacks on the line-side (aggregate data stream) and on each terminal interface on the user side of the multiplex. Modern multiplexers include built-in remote control loopbacks and many include built-in test message generator/receivers for test purposes.

c. When the networks include asynchronous/isochronous crypto devices some of the fault-isolation methods discussed for a synchronous secure network cannot be used since these cryptos do not perform the automatic sync detection and re-sync functions that are performed by the CAU/sync cryptos. The asynchronous/isochronous cryptos do include a front-panel control which permits operation in the plain text mode. In this mode the encryption circuitry is essentially by-passed and fault-isolation can be accomplished. However, this operation requires action by crypto personnel at both ends of the circuit which clearly violates our objectives. Another solution to this problem is to provide either an external manually operated loopback capability for the terminal side of the remote crypto (with the control located at the terminal) or an external remote controlled loopback. The send/receive clock phase difference problem does not exist here since the terminal side is operated in an asynchronous mode.

d. If the discussions in Sections 2.0, 3.0, and 4.0 seem to belabor what may be obvious issues to many readers, such was done purposely to be able to argue conclusively that an exotic, expensive, complex and difficult to operate dual-ended facility is not required to meet the objectives of a fault-isolation capability which can isolate faults in a base level data network down to the "which vendor device/link"? There is much literature on the subject of network fault-isolation which imposes requirements to monitor/measure almost every possible parameter which can be measured and these requirements are imposed without analysis of what problems are to be isolated, to what level, and by whom (skill level).

e. Based on the fault-isolation methods discussed in this paragraph (4.9), there are some requirements/methods which must be added to those discussed in paragraphs 4.1 through 4.8.

(1) Each test used to isolate problems required comparison of the observed/measured results with the results of the same test performed when the circuit was operating normally. Thus, a set of normal values with permissible deviation limits must be established for each circuit as part of the cutover and acceptance procedures. These values should be compiled as part of a set of fault-isolation trees similar to Figures 3-1, 3-2, and 3-3 for each different circuit configuration.

(2) The requirements for a modem handshaking monitor discussed in paragraph 4.3 were based on the EIA RS-232C non-secure interface. In the fault-isolation discussions for a synchronous secure network, there is a requirement to monitor the status of the "loss of carrier" lead between the processor end CAU and modem, the "data inhibit" and "sync initiate" leads between the processor and CAU, and the master and remote alarms on the CAU. The modem handshaking monitor needs to have this capability.

(3) All synchronous cryptos should be equipped with CAU's (excluding new generation devices) which perform the automatic sync functions.

(4) All asynchronous/isochronous cryptos should be equipped with the applicable mod kit or auxillary device to permit clear text operation or preferrably, an external loopback device should be installed.

5.0 COMMERCIALLY AVAILABLE DEVICES.

5.1 Built-in Loopbacks.

a. Many modem and multiplexer manufactures offer built-in loopback arrangements, some of which can be remotely controlled. Various signaling schemes are used; for example, in the Lenkurt 263A Wireline Modem, the processor end modem loopbacks are exercised by front-panel switches on that modem. A front-panel switch on this modem will also activate either a signal line or digital loopback at the terminal end modem. Signalling to the distant modem for the digital loopback is via a bi-polar violation code; signalling for a signal line loopback is via reversing the polarity of the bias current on the signal line. In the Codex 8200 series wire line modems, the remote digital loopback is activated by off-setting the signal voltage levels. General Data Comm Industries modems and multiplexers use a digital message block to activate remote loopbacks, which for use in multipoint networks, includes a unique address for each remote modem connected to the common signal line.

b. Some modem/multiplexer manufacturers have extended the remote loopback capability so that it can be activated for any network channel from a centralized control panel. This control panel may also activate other special tests. In the General Data Comm Industries network diagnostic control system, an optional remote control circuit card is added to each modem. Also offered is an external remote control device for use with other vendor's modems. Thumb-wheel switches are used to set up the remote modem address and a second thumbwheel switch is set for the desired loopback (line side or digital). When the command button is depressed, the unique message block is transmitted, including the modem address. The signalling technique used is designed for transmission over extremely noisy paths and the addressed modem makes a positive response indicating that the command has been received and executed. The central control panel provides for connection of external test equipment as well as providing a built-in BERT capability. The network control can also be extended to handle multiplexer channels. The Codex network control system also adds a remote control P.C. card to each remote modem. Commands to remote modems include a unique address for each modem on a multipoint channel; they are transmitted via a narrow band (within voice channel) FSK signal and thus can be used while normal data is flowing. In addition to remotely controlled loopbacks, the system performs BER tests in which one-way tests (without loopbacks) are possible. The remote control card in the remote modem compares the received test pattern with the proper pattern, which is stored in the modem, and reports the number of errors back to the central unit. The ICC/MILGO network diagnostic control system also uses an FSK narrow-band channel (within the voice channel) for remote control signalling and provides for BER testing via loopbacks or between modems.

c. Data Products of New England offers an external control module for use with any modem or multiplexer which provides a remote controlled digital loopback. The unit is inserted at the remote digital interface, and where required for multipoint operation, can be programmed to detect a unique address. The remote loopback is activated by signalling over the normal data path and the command message can be initiated by any pattern generator (part of a BERT set or distortion analyzer) which provides for setting up of unique character bit codes. The limitations here are first, there is no line-side remote loopback provided, and secondly, the commands require that both modems and the transmission path be at least marginally operational. It does, however, provide the capability to do loopbacks with secure channels which contain the AN/UYK-22 CAU. A remote control module can be inserted on both sides of the CAU/crypto with a different address assigned to each device. The remote control unit is equipped to accept two status indicators from the CAU and to accept a remote command to re-set the CAU.

d. The foregoing discussion by no means covers all of the available modems, multiplexers, or external devices which can provide remotely controlled loopbacks. It is meant to show that these functions are readily available off-shelf.

e. As previously discussed, use of line-side loopbacks depends on using modems and transmission paths in a 4-wire full-duplex configuration even though the processor/terminal may operate in a half-duplex mode (alternate send/receive).

f. The important point is that the capability to remotely activate both digital and line-side loopbacks must be designed into the network and procurement specification documentation for modems and multiplexers must include these requirements. Devices including these capabilities cost little more than those without them and cost less than adding the capability externally.

5.2 Patching/Switching. As discussed in Section 4.0, the primary advantage of patching over switching is cost; and if modem, crypto, and multiplex swapping, and circuit alt-routing are required in addition to monitor and test functions, patching is even more economical. The primary advantage of switching is the ease of operation and less chance for error as compared to the operator under pressure handling a maze of patch cords. However, both are readily available in configurations specifically designed for processor oriented communications subsystems.

a. Dynatech offers a family of digital patch modules which have been widely used in the Air Force for patch and test facilities. Each comm channel jackset contains a monitor jack, equipment jack and line jack. This configuration permits monitoring, testing and equipment/channel swapping. For EIA RS-232C channels, either 12 or 16 conductor jacksets are available (the 12 conductor set also meets the MIL STD 188/crypto interface requirement). The jacksets are configured on a standard 19" rack mounting panel with either 12 or 16 jacksets per panel. Additional standard audio jacksets are required for the modem line-side interface and these can be mounted on the same panel as the digital jacksets or on a separate panel. They also offer a hybrid patch switch module which uses patching for monitor/test purposes and switching for modem/processor port channel swapping. Some configurations also provide LED's to indicate the status of the modem handshaking leads.

b. International Data Sciences offers both patching and switching [illegible]. A good feature of both configurations is the modularity. Each comm channel jack set or switchset is self-contained in a plug-in module. A standard card-cage with power supply permits adding different types of modules, as they are required. The patch modules also have a safety feature in that insertion of a patch cord in a channel jack does not swap/disconnect the equipment unless a safety switch is also activated. A hybrid configuration is also offered which uses switching for modem/channel swapping and patching for testing. The jack set modules monitor two of the interface leads with LED's (receive data and carrier detect), while the switch modules can be extended to monitor 12 leads with LED's. Audio patch modules can be added to the digital side configuration or configured separately.

c. T-Bar Inc. offers a family of switching modules specifically designed for processor-end monitoring, testing and equipment/line swapping. The switching matrix is modular (per channel) and is controlled from a single control panel. The desired channel is dialed-up via thumb-wheel switches and the desired action (monitor, test) is activated via pushbutton controls. Some configurations provide only monitor/test switching, while others include equipment/line swapping. The EIA RS-232C interface leads are monitored by LED's. T-Bar also offers switch modules for remote terminal locations which can

perform loopback/switching functions under control of the processor-end control panel. Commands are encoded and transmitted over the normal transmitter path using narrow-band FSK signalling.

d. ADC Telecommunications also offers switching in modular form for monitor/test functions. A central remote control panel is used to address the desired channel and activate the mode (monitor/test) desired. The channel being accessed and its status are displayed. Switching access modules consist of relays mounted on PC boards which plug into a standard card-cage.

e. Again, the foregoing is not a complete review of available patching/switching capabilities. It merely serves to establish the fact that such devices are off-shelf in configurations which meet the requirements established in Section 4.0.

5.3 Modem Handshaking and Processor/Terminal Protocol. The requirements to monitor and emulate modem handshaking at the processor end also include the requirement to monitor/emulate the status of certain control leads in both secure and non-secure synchronous configurations in which modem handshaking per se does not occur.

The reason for pointing out this difference is; if a network does not include channels over which actual modem handshaking occurs, then the control lead monitor/emulator does not have to include a timed sequence capability. It need only provide a means to indicate the present status of each lead and the capability to apply/remove control logic voltage to each lead. In the discussion on patching/switching it was noted that this capability is available in off-shelf patch/switch devices. It is also available in many pulse distortion analyzers and BERT devices.

The devices discussed here include the time-sequence capability; these devices also include the processor/terminal protocol capabilities.

a. Data Products of New England call their device "Step 21, Data Link Tester and Exercisor". Operator interface is via an octal (or hex) keypad and uniquely defined keys. The display is limited to 64 characters of alphanumeric, octal or hex representation of ASCII, EBCDIC or Hex codes. Non-printable control characters are displayed as english words (abbreviations). The operator can scroll through the 1000 character buffer (one or 16 characters at a time). The unit can monitor and emulate (processor and terminal) time sequenced modem handshaking routines. The unit has the BISYNC, SLDC and HDLC protocols preprogrammed and contains storage for 15 user programs. It can store 64 characters before a programmed event and 1000 characters after that event for subsequent analysis. In addition to modem handshaking and processor/terminal protocol, the device also contains a BERT capability and a pulse distortion analyzer (peak distortion). The BERT does not have an adjustable sampling window which is required for time skew detection on synchronous channels.

b. Halcyon offers their Model 803A Data Link Analyzer which provides a hexadecimal keypad, 24 special function keys and a 256 character display. The display also permits split screen operation; i.e. simultaneous display of both directions of transmission. The unit can monitor and emulate (processor and terminal) time sequenced modem handshaking routines and can handle several preprogrammed protocols plus user generated programs (1K to 4K bytes in program buffer). The capture buffer is 4K bytes with 2K allocated to data and 2K allocated to handshaking lead status. The operator can scroll through the capture buffer; the transmit data is displayed in normal video, receive data in reverse video, and errors are dimmed. A tape cassette option is available for storage of test and monitoring results. ASCII, baudot EBCDIC, hexadecimal, IBM Selectric and 2740/41 codes are preprogrammed.

c. The International Data Sciences Data Trap uses a hexadecimal keypad and a 512 character display as the primary operator interface. The operator can scroll through a 4096 character capture buffer; the buffer/display can also be operated in a split screen mode (simulatneous send/receive monitor). The device can monitor/emulate timed sequence modem handshaking and is preprogrammed for BYSYNC, SDLC, HDLC, ADCCP and X 25 processor/terminal protocols; other protocols are available as preprogrammed options. Baudot, ASCII, EBCDIC, Selectric, Hex and Octal codes are standard. It will automatically store data (in either or both directions) after a preprogrammed event (character string).

d. Dynatech Data Systems offers their programmable data communications monitor/simulator which uses an alphanumeric keyboard (similar to 64 character ASCII) and a 512 character display for operator interface. The device can monitor/emulate time sequence modem handshaking routines and is programmable (1K BYTE) for processor/ terminal protocol monitoring and simulation. The capture buffer is 4046 characters plus parity and handshaking lead status. A tape cassette is included which provides additional storage of 200K characters plus parity and lead status. ASCII, EBCDIC and Hex codes are standard with options for a total of 6 codes. The device will store 256 characters following a preprogrammed event and approximately 200 characters preceeding the event. It also contains BERT (without an adjustable sampling window) and peak pulse distortion measuring capabilities.

e. The Atlantic Research Corp. Intershake Test System provides an ASCII keyboard and 1024 character display as the primary operator interface. The device can monitor/emulate time sequence modem handshaking routines and is programmable (15 programs) for monitoring/emulating processor to terminal protocols. The keyboard and display can be operated in the ASCII, Hex, EBCDIC, and EBCD codes. The 1024 byte capture buffer will trap data based on recognition of a specified event. An optional cassette tape unit provides 500K bytes of storage plus event markers. The unit accomplishes both pseudo-error rate (parity counts) and real BER tests, but does not have an adjustable sampling window.

f. The Digitech Data Industries ENCORE 100 provides an ASCII keyboard and 896 character display as the operator interface. It can monitor/simualte modem handshaking routines and is programmable (8 to 24K bytes) to monitor/simulate processor to terminal protocols. Programming is accomplished in a modified form of basic. The capture/trap buffer provides 20K bytes of storage and an internal tape unit provides 500,000 bytes of additional storage. A maximum of 8 codes can be handled with ASCII, EBCDIC, BCD, and Selectric as standard. The unit accomplishes parity oriented, BER and character-error-rate tests, but does not have an adjustable sampling window.

g. The competition in the market for these devices has grown dramatically with the advent of the microprocessor and the large increase in on-line processor systems. This review covers only a few of the devices offered and each month brings one or two more. This means that we should be able to obtain these functions in almost any configuration required.

5.4 Error Tests and Pulse Distortion Measurements. Most of the handshaking/protocol monitor/emulators provide the required error detection and analysis capabilities (parity oriented and BER) with one exception; i.e. an adjustable sampling window which is required to accomplish a pseudo-timing/data skew test on synchronous channels. Some of the devices also include a pulse distortion measurement capability. But this is limited to the send/receive data leads, whereas a requirement exists on synchronous channels to accomplish pulse distortion measurements on the send/receive clock leads as a pseudo-jitter measurement.

a. There are many pulse distortion test sets available, but all are designed for operation by the highly skilled maintenance technician and include capabilities far beyond the requirements discussed in Section 4.0. It would appear that a simple selector switch (hardware or firmware) could be added to the monitor/emulators to provide the capability to measure peak pulse distortion on the clock leads as well as on the data leads, and we will proceed on that assumption.

b. BERT devices also abound in the marketplace, however, only two could be identified which provide an adjustable sampling window; i.e. the Digitech Data Industries, Inc. Model 2000 Series Bit Error Rate Tester and the Sierra/Philco Model 1914C Data Transmission Test Set. Both of these instruments, however, are designed for operation by skilled technicians versus our operator fault-isolation objective.

c. The programmable monitor/emulator devices which accomplish pulse distortion measurements, do so in software (firmware) by sampling each incoming pulse a large number of times, counting the actual number of samples obtained between the leading and lagging edges of the pulse, comparing this number against the proper number (perfect pulse) and computing the difference as a percentage of a perfect pulse. This same software could be adapted to provide an adjustable sampling window for use with Bit Error Rate Tests; i.e. the operator could select the percentage of the pulse to be considered which in turn would limit the number of samples to be considered by the BERT decision circuitry. The samples to be considered are equally distributed on both sides of the clock pulse. A skewed data pulse would then appear as having too many samples on one side of theoretical center pulse (the excess is ignored) and too few on the opposite side. The adjustable sampling window is thus the specification of how many less than normal samples are to be accepted? A pulse with less than the specified minimum number of samples is counted as an error.

d. The capabilities of measuring peak pulse distortion on the clock leads and making a pseudo-clock skew measurement with an adjustable sampling window BERT are only required on synchronous circuits, and on these circuits are only required to isolate crypto versus modem problems; the number of faults attributable to clock pulse jitter and clock/data skew are probably small in the on-base wire systems being considered here. Thus, if the cost of adding these capabilities to off-shelf emulators is great, it would probably not be cost effective to include them and certainly would not be cost effective to add separate distortion analyzer and BERT test sets; especially in view of the fact that the crypto room maintenance is equipped with a dual-trace scope which is capable of making these measurements (by a technician) if they are absolutely required to isolate a fault.

5.5 PAR/Level Measurements. Only two sources could be located for a PAR meter; one used in the Bell System and one produced by Marconi Instruments (Model TF 2809 Data Line Analyzer). The Marconi instrument includes signal level and noise level measurement functions in addition to the PAR function.

5.6 From the foregoing discussion it can be concluded that the devices required to extract and analyze the information, needed to isolate network faults, are available from industry as off-shelf devices. In the next section a "bare-bones" fault-isolation facility will be constructed.

6.0 A "BARE-BONES" FAULT ISOLATION.

6.1 Requirements Review.

6.1.1 Loopbacks.

a. All communications paths (including modems) to be operated 4-wire full-duplex, even if terminal operates in a half-duplex mode.

b. All modems and multiplexers to include user-side and line-side loopback capability. When located external to the fault-isolation facility, loopbacks to be remotely activated from the fault-isolation facility.

c. External remotely operated digital loop-back devices to be inserted between KW-series teletypewriter crypto's and the user terminal.

6.1.2 Patching.

a. Patch panels are selected over a switching matrix primarily because of cost considerations. The capability to use a switching matrix in an automated scanning mode is not a requirement for the on-base computer system. This capability does have advantages for large (hundreds of channels) trunking networks which consist of many nodes, repeaters, mux-demux points, etc. In these networks continuous scanning (measurement and comparison against some threshhold) can provide the means to detect gradual degradation (trending) in performance. However, for the predomenently on-base wire path computer network, such analysis is not warranted.

b. The digital-side patching must provide the following capabilities:

(1) Access circuitry for 12-leads for each channel (send data, receive data, send timing, receive timing, signal ground, shield, plus six control leads).

(2) A monitor jack for each channel to provide for bridging each of the leads for monitoring purposes.

(3) An equipment jack for each channel which permits seizing the channel and testing back toward the central processor.

(4) A line jack for each channel which permits seizing the channel and testing out toward the remote terminal.

(5) The equipment and line jacks are "normal-through" circuitry; i.e. the channel leads are connected through the jack-sets when no patch-cord is connected. Insertion of the patch cord opens the "normal-through" connection and thus permits connection of test devices to the channel. By cross-patching (the equipment-jack of one channel to the line-jack of another channel), modem swapping can be accomplished (with a similar patch arrangement on the analog side of the modems).

c. Following are some desirable capabilities to be included in the digital side patching:

(1) A standard method of connecting the central processor communications channel leads through the patch circuitry. Most processors use a channel adaptor card which is designed to use the 25-pin connector and lead arrangement specified in EIA

Standard RS-232C. It would be advantageous to also use the RS-232C connector on the patch panel (rear-processor side connection) as the means to connect the processor channels. Another advantage here is to hard-wire (at factory) the 12 leads (out of the 25 on RS-232C) from the connector through the patch circuitry in a standard manner (i.e. the same function is always on the same lead for all interfaces). This allows the connection of test devices to be made in the same way for all channels.

(2) A set of three LED's for each channel; one to provide an indication of activity on the send data lead, the second for the same purpose on the receive data lead, and the third to be capable of being connected to any of the remaining leads or to an external circuit (such as a crypto alarm circuit).

(3) A single set of 11 LED's connected to a patch jack. Patching between this jack and the monitor jack on any channel then provides a quick-look status of active leads.

(4) Test-jack(s) for connection to digital test device(s).

d. The analog-side patching must provide the following capabilities:

(1) Access for 4-wires for each channel.

(2) A monitor jack for each channel.

(3) An equipment jack for each channel.

(4) A line jack for each channel.

(5) Test jack(s) for connection to analog test devices(s).

6.1.3 Digital Test Device.

6.1.3.1 Modem Handshaking: The requirements are:

a. Programmable timed sequence monitoring, emulation, display and storage.

b. Programmable lead status change monitoring, display and storage (in conjunction with monitoring, display and storage of send and receive data streams).

c. Measurement of time elapsed between handshaking events.

d. Playback of stored lead status in conjunction with stored data stream.

6.1.3.2 Processor/Terminal Protocol.

a. Programmable Monitoring Display, and storage of both directions of transmission simultaneously (in conjunction with handshaking lead status).

b. Programmable emulation, display, and storage of both processor and terminal routines.

c. Display non-printing control characters.

d. Handle line codes using 5, 6, 7 and 8 bit characters, plus parity and start/stop pulses as required for ITA #2 (American and CCITT), ASCII, ITA #5, BCD and EBCDIC.

e. Playback of stored data streams (in conjunction with handshaking lead status).

f. Capture/trap selected data based on recognition of programmable character code/sequences.

g. Measure time elapsed between programmed events.

h. Operate at all $75x2^N$ line speeds up to 19.2 Kb/s plus 50 Kb/s.

6.1.3.3 Traffic Errors.

a. Monitor, display and store data streams in both directions of transmission.

b. Trap/capture, display and store selected data based on recognition of programmable character codes/sequences.

c. Provide roll/scroll through three pages (512 characters per page minimum).

d. Playback of stored data (in conjunction with handshake lead status).

e. Handle line codes and speeds per 6.1.3.2d and h.

f. Provide for programmable test messages.

g. Handle character and block parity schemes including vertical and horizontal redundancy checks, and cyclic redundancy checks. Count, display and store number of parity errors and ARQ's.

6.1.3.4 Digital Signals.

a. Peak and average pulse time distortion; switchable to send data, receive data, send clock and receive clock leads.

b. Bit Error Rate Test with an adjustable sampling window in the receiver/error detector.

6.1.3.5 General.

a. ASCII keyboard for programming and commands. In conjunction with the video display, to be capable of operating in a conversational mode with a distant terminal in line codes and speeds per 6.1.3.2d and h.

b. Video display consisting of a minimum of 512 characters.

c. Operate in half and full-duplex, asynchronous and synchronous modes.

d. Provide both RS-232C and MIL STD-188-100/114 digital interfaces.

e. Provide for digital patch panel connection to the monitor, equipment and line jacks via the test device jack circuit.

6.1.4 Analog Test Device.

a. PAR test via loopbacks.

b. Signal level in Dbm.

6.1.5 Fault-isolation Facility Configuration.

a. All patch panels and test devices to be installed in a common location (subject, of course, to red/black criteria for secure installations); i.e. the practice of locating the red digital patch within the central processor configuration, the black digital patch in the crypto room, and the analog patch in a modem/cable room does not provide for a network fault-isolation facility. It provides three maintenance patch and test facilities instead.

b. All modems and multiplexers must also be installed in the same location as the patching/test devices. This is necessary to provide easy access to local and remote loopback controls. It also permits the operator ready access to the various status/alarm indicators on the modem/multiplex devices.

c. In a secure facility requiring use of RFI cabinets, it needs to be determined (by Tempest test) if the cabinets in the fault-isolation facility (patch, test device, mux, modem) can be operated without front-doors or provide RFI treated viewing slots in these doors which permit viewing of the patch panel lead status indicators and the modem/mux device status/alarm indicators.

6.2 The Network Scenario.

For the purpose of costing the "bare-bones" fault-isolation facility, the following base data network is assumed:

6.2.1 Central Processor Comm Front-End.

a. Consists of 48 user channels.

b. All channels send/receive classified information.

c. The channels operate in various modes (half/full-duplex, sync, async), line codes and speeds.

6.2.2 Remote terminals: Of the 48 remote terminals;

a. Twelve are full-duplex and are located in different buildings on the base and each is protected with a KG-series/CAU crypto configuration.

b. Twelve are full-duplex and are located in groups of four; i.e. each group of four is in a secure area in a different building from the other groups. Each group of four is multiplexed into a common bit stream and this bit stream is encrypted via a KG-series/CAU configuration.

c. Twelve are full-duplex and are located in different buildings on the base and each is protected with KW-series crypto.

d. Twelve are half-duplex and are located in different buildings on the base and each is protected with KW-series crypto.

6.3 The Fault-Isolation Facility/Costs.

6.3.1 Loopbacks.

a. The additional cost of providing 4-wire full-duplex modems and wire paths for the twelve half-duplex terminal/crypto configurations is simply the cost of the second wire pair since the cost of low-speed full-duplex modems is equal to, or less, than the cost of half-duplex modems. A typical cost for an on-base wire pair is estimated to be $6.50 per month. Over a ten-year life cycle, the cost of the twelve additional pairs is estimated at (6.50 x 12 months x 12 pairs x 10 years) $9360.

b. The additional costs, of providing internal remotely operated loopbacks for all terminal end modems and multiplexers and external remotely operated digital loopback devices for the terminal end KW-series cryptos, are as follows:

(1) Twelve full-duplex KG-series channels; $250 per modem or $3000.

(2) Twelve, in three groups of four terminals, each multiplexed and using KG-series devices: 3 modems at $250 each is $750. 3 multiplexers of 4 channels each at $250 per channel is $3000 for a total of $3750.

(3) Twelve full-duplex KW-series channels: 12 modems at $250 each is $3000. 12 external digital loopback devices at $500 each is $6000 for a total of $9000.

(4) Twelve half-duplex KW-series channels; same as full-duplex KW-series; $9000.

6.3.2 Patching.

a. Red-Side: 48 terminal channels plus 4 multiplex data streams (including all features described in 6.1.2) is aproximately $5500.

b. Black Side: 36 terminal channels plus 4 multiplexed data streams is approximately $4000.

c. Analog: 36 terminal channels plus 4 multiplexed data streams is approximately $2250.

d. Racks/Cabinets:

3 RFI cabinets at $3000 is $9000.

6.3.3 Digital Test Device.

A device having all of the features listed in 6.1.3, except for switching the pulse distortion measurement to the clock leads and providing an adjustable sampling window in the BERT receiver costs $12,500. The addition of these features (in production quantities) would raise the price to approximately $15,000.

6.3.4 Analog Test Device.

This device is available at a cost of approximately $3000.

6.3.5 Bare Bones Facility Cost Summary (All Costs Rounded Off).

Additional pairs for half-duplex channels		$9500
Remotely Operated Loopbacks		25000
Patching, Red		5500
Patching, Black		4000
Patching, Analog		2300
Patching, Cabinets (RFI)		9000
Digital Test Set		15000
Analog Test Set		3000
	Total Cost of Equipment	$73,300
	Engineering/Installation:	7,500
	Total Estimated Cost:	$80,800

7.0 THE "PAYBACK"

7.1 Channel Outage Time.

a. Studies conducted by one vendor (1), indicated that the average channel outage time lasts for six hours, of which four or more are spent in a finger pointing exercise among the system operator and the various vendors. This study also indicated that each channel failed on the average of once-per-month.

b. In the 48 channel scenario network used in 6.0 the total yearly channel outage time would be (6 hrs/month x 48 channels x 12 months) 3456 hours.

7.2 Channel Outage Tangible Costs.

a. In terms of the central processor facility shift-supervisor (assumed to be the one engaged in the 6 hrs of finger-pointing and channel restoration), the 3456 hours equates to about two manyears; at a cost of approximately $40,000.

b. In terms of idle terminal, modem, multiplex and communications lines, based on an average monthly leased costs, equates to approximately $10,000 for the 3456 hours of outage.

c. In terms of idle processor and communications front-end time, based on average monthly leased costs, equates to approximately $6000 for the 3456 hours of outage.

d. Total tangible costs of outages $56,000.

7.3 Payback with Tangible Costs of Outages.

a. Cost of 48 channel scenario facility $80,800

b. Of the $56,000 in tangible costs, approximately 2/3rds can be saved with the barebones fault-isolation facility just by eliminating the finger-pointing exercise;

2/3 x $56,000 = $37,333

c. Payback period equals $80,800 ÷ $37,333 or slightly over 2-years.

7.4 Intangible Outage Costs.

These costs included delayed and lost data, unhappy customers and the purging of errors inserted into the system due to the outage. Also included is the cost of providing some type of service to the user during the outage. We have no way of assessing dollar costs for these items.

7.5 Conclusions.

7.5.1 Meeting of Objectives.

The foregoing study shows that, by using remotely activated loopbacks on all channels, by providing digital and analog patching at the central facility, and by providing a single digital and a single analog test device, we can provide a base level data network fault isolation capability which is single-ended (i.e. all operations performed at the central processor location) and which can be operated by senior computer operator personnel.

7.5.2 The Value.

a. One may argue for different facility costs based on smaller or larger networks, or a different mix of kinds and types of channels, all of which would change (increase or decrease) the estimated cost of about $1700 per channel used for the scenario network.

b. One may also argue for different costs for the idle equipment/circuit time based on a different set of processor facility configuration assumptions, which would change the cost of the outage time.

c. And, of course, one may argue for a different number of outage hours per channel as well as the portion of those hours saved with such a facility.

d. However, if reasonably realistic figures are used, it is believed that the payback period will be a reasonable one (less than 3 years), and will justify the acquisition costs.

e. In addition, the intangible benefits, including better and more efficient service to the users, must be given some weight, depending on the importance of the information being handled.

REFERENCES

(1) Weaver, T. H., Internal Report, Digitech Data Industries, Inc., 1972

(2) Doll, Ed., "Three Domains of Data Communications Testing", NTC '76 Proceedings (IEEE).

(3) Campbell, L. W., "The PAR meter: characteristics of a new voiceband rating system", IEEE Transcom, Vol. COM-18, No. 2, April 1970.

(4) AF Technical Order 31S5-2UYK22-1, "Technical Manual for Crypto Auxiliary Unit (CAU).

(5) Technical brochures from various vendors of patching, switching, modem, multiplex and test devices.

DISTRIBUTION

ORGANIZATION	NO. COPIES
HQ AFCC/ EPE	1
EPP	1
EPPB	1
XOP	1
XOD	1
XOY	1
SA	1
LGY	1
CDO	1
CDM	1
CDX	1
FFO	1
NCA/EIEXR/DMO	5
EIE	5
EIEGC	1
EIEGD	1
XO	1
LG	5
SCA/EIEXR/DMO	1
EIE	1
EIEGB	1
EIEGD	1
XO	1
LG	1
ECA/LG	1
XR	1
DO	5
PCA/EIEXR/DMO	1
EIE	1
EIEGD	1
XQ	1
LG	1
DO	1
SACCA/DO	1
LG	1
XQ	1
TACCA/XP	1
LG	1
AFCCPC/CC	1
SKX	4
SKB	1
1842 EEG/EEI	1
EEIC	1
EEICT	1
EEICB	1
EEICS	1
EET	1
EETS	1
EETSC	1
EETST	


DA
FIL